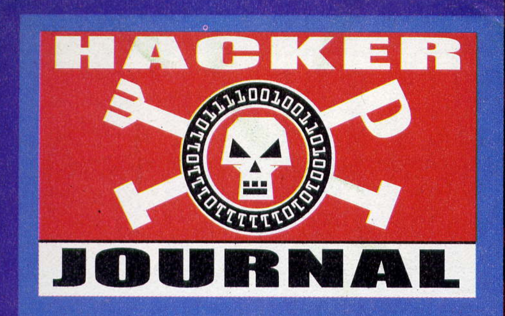

TODO LO QUE NADIE HA OSADO DECIRTE ANTES
HACKER
JOURNAL
PLAYSTATION2
NO LIMITS!
RECURSOS PARA JUGAR CON TODO
2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN Y ARTÍCULOS
00012
8 413042 435235
FIRMAS EN 3-D
FIRMAMOS EN RELIEVE...
TOP SECRET
AES: EL ALGORITMO DE CIFRADO DEL GOBIERNO DE EE.UU.
STOP SPAM!
LOS SECRETOS DE LOS FILTROS
¿YA HAS PROBADO FREEBSD?



Año 3 - N. 12 - 2005

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Amadeu Brugués, Eric Sala, Infoambiente, Gualtiero Tronconi, Eduardo Bracaglia, Gregorio Peron, Contents by MDR

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3dO, Eric Sala, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico:
info@dopla.com

Redacción
SPREA EDITORI
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Distribución
SGEL - Avda Valdelaparra 29
Poligono Industrial De Alcobendas
Madrid - Spain

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack·er (hăk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

ALTERNATIVAS FIABLES

Seguridad y libertad: una perpetua dicotomía. La seguridad es fundamental para que nuestro uso de la red sea razonablemente productivo. Sin embargo, fácilmente las medidas de seguridad pueden utilizarse en contra de los propios usuarios, limitando su libertad y privacidad. Internet es un campo de batalla privilegiado de esta importante batalla.

Es por ello que en este número nos interesamos especialmente por el proyecto FreeNet. Se trata de una propuesta ya en marcha para conseguir algo de privacidad en la Red de redes. A diferencia de los programa peer to peer, no se trata sólo de intercambiar programas o contenidos. FreeNet va más allá, proponiendo un uso de la red en el que la privacidad es primordial.

La propuesta de FreeNet es interesante también porque vuelve a los orígenes de Internet. En efecto, todos los usuarios de FreeNet ceden parte de su espacio en disco para conservar los contenidos de la red. Estos contenidos están cifrados, de modo que el usuario no tiene forma de saber qué contiene exactamente su propio disco. Esta estructura es esencialmente descentralizada para hacerse más resistente a los ataques, provengan de donde provengan.

No nos resistimos a reproducir aquí la frase de Mike Godwin: "Me preocupa mi hija e Internet cada vez más, aunque sea aún d e m a s i a d o pequeña para conectarse. Me preocupa que dentro de diez o quince años vendrá y me dirá: papá, ¿dónde estabas cuando nos quitaron la libertad de expresión en Internet?". Si queremos garantizar las libertades del futuro, ahora es el momento de hacer algo...

redaccion@hacker-journal.com

UNA REVISTA PARA TODOS



NEWBIE



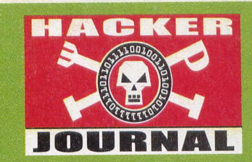
MID HACKING



HARD HACKING

El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).

SUMARIO



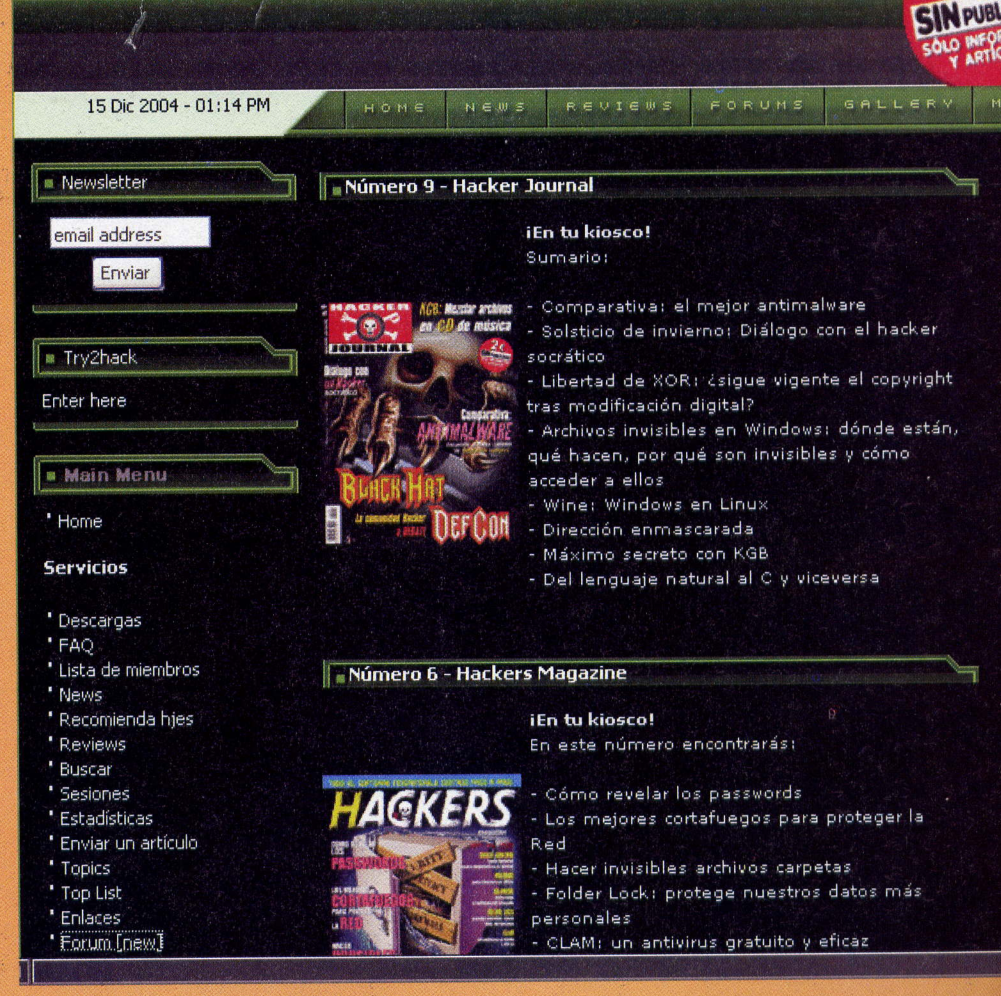
SITIO WEB

Como en cada número de Hacker Journal, os recordamos que tenéis a vuestra disposición el sitio web de la revista, www.hacker-journal.com, para seguir leyendo y aprendiendo sobre el Hacking. Recordad también que disponéis de los foros donde podéis exponer dudas y preguntas, observaciones, etcétera. Todos los visitantes del sitio web colaborarán en hallar respuesta a todas las preguntas. ¡Entre todos lo conseguiremos!

Visita nuestro sitio web:
www.hacker-journal.com

CODIGO DE LA SECRET ZONE
user: secreto12
password: doc3n4









mailto:

redaccion@hacker-journal.com

ARTICULO REPETIDO

Me llamo Jorge y soy un lector de su revista entusiasmado con casi todas las secciones de su revista. El día uno de marzo compré su nuevo ejemplar, el número 11, donde al ojear las páginas durante las clases me llamo la atención de que uno de los reportajes ya se incluyó en el pasado número sobre bluebugging, al pensar que podía ser una continuación la leí atentamente descubriendo que era el mismo artículo.
Les agradecería que me informaran si es un error de mi revista o suyo ya que guardo las revistas y no me gustaría tener un ejemplar defectuoso.
PD: perdón por las posibles faltas ortográficas

JORGE

Apreciado Jorge, efectivamente el artículo sobre el Bluebugging se publicó de forma repetida, por error. Desde aquí pedimos disculpas a nuestros fieles lectores, y nos comprometemos a poner más cuidado para evitar la repetición de este suceso.



CHIP DE IDENTIFICACIÓN

Hola a tod@s, y sobretodo a los redactores de esta magnífica revista!!!
Realmente que quedé impactado al leer sobre lo del chip subcutaneo que comentasteis en el úlitimo numero... Creo que este chip no es simplemente una nueva forma de ir a comprar, sino que es más bien una nueva forma de invadir nuestra privacidad. ¿Que pasaría si el estado lo utilizara para saber donde estamos o que hacemos? Prefiero hacer cola, que no que me controlen, porque ya lo veo yo... Dentro de unos años, si el proyecto tiene exito, será como el DNI, y obligatorio. Realmente sería como en MATRIX... y me niego ponerme una cosa de estas en mi cuerpo. Eso si.... seria divertido descubrir si hay alguna forma de hackearlo!

PATRUSQUITO

Compartimos el repeluz ante un chip de este tipo. Por el momento no parece razonable que se llegue a tal exceso, pero por si acaso vale la pena mantenerse al corriente de los acontecimientos. Bajo la cobertura de presuntas ventajas, los potenciales inconvenientes son innumerables... Y no es difícil imaginar los usos asociados a la "seguridad" que una forma de gobierno con pocos escrúpulos podría obtener de un artilugio así.

HACKER Y DELITO

Hola buenas soy D3F3nd3r
Ya os escribi pero komo no me habeis respondido lo vuelvo a intentar :)
Os felicito por al revista!
Os he escrito para deciros ke toi intentando crear un ejercito de zombis, el programa trata de dos partes el servidor i el cliente, todos los zombis se conectan a un servidor i yo me puedo conectar a este servidor desde cualquier sitio por msdos y modificar la ip a la que atacar, comenzar un atake a una web o a un pc... solo tengo una preguntas... soy nuevo en este mundo por lo tanto las preguntas os pueden resultar estupidas.
¿Me pueden pillar si me konecto a traves de un cyber?
¿Si me pillan ke hacen?
¿Se puede conseguir algun servidor ke este 24h conectado i ke sea gratis donde puedas ejecutar un programa?
¿Los zombis para atacar un pc que tendrian que hacer pings? y para una web, conectarse y actualizarla todo el rato?
¿kuantos pcs tendrian que ser para ir bien?
Y ahora un cosa ke la pregunto mas por curiosidad ke por otra cosa yo ya e echo muchas web y siempre pongo eso tipiko de "esto es solo kon fin educativo todo el material aki expuesto..blablabla.." o si creo un virus y se lo passo a alguien ke sabe lo ke es y ese lo difunde kien es el responsable yo por crear el prog o el por difundirlo?
¡Gracias por todo! y sobretodo por hacer una revista asi y...sin publicidad pk una kosa ke odio de otras revistas es la publicidad..

D3F3ND3R

Lo hemos repetido varias veces, pero no nos importa insistir cuantas veces sea necesario: desaprobamos radicalmente todo tipo de conductas y proyectos encaminados a causar molestias o daños a otros usuarios y, en general, a todas aquellas iniciativas que pretenden infringir la ley.
Así las cosas, la creación de un ejército de zombies para atacar equipos nos parece lamentable. Es cierto que un buen hacker debe conocer estas técnicas para preparar defensas adecuadas, pero atención, su metodología es radicalmente distinta: en primer lugar, hace sus experimentos en una red privada y cerrada al mundo exterior, para evitar accidentes. Y en segundo lugar, aprovechará la experiencia para preparar contramedidas, nunca para expandir su propio ejército.
Créenos: olvídate de usar cybers y otras zarandajas y, si quieres aprender, que sea con seguridad y nobles intenciones. De lo contrario, puedes encontrarte con graves problemas legales, y desde luego conseguirás cosechar la antipatía de la comunidad de usuarios. No es la mejor medalla que puedes conseguir, no te quepa duda...
Respecto a los virus, debes ser extraordinariamente cuidadoso. Si tienes un virus aislado y lo pasas a alguien que no sabe manejarlo apropiadamente, puede desencadenarse una infección. Y desde el punto de vista legal, si procede de ti de algún modo, no descartes verte implicado en los procesos que puedan llevarse a cabo. Manejar virus, gusanos, troyanos y demás es un procedimiento delicado, y el peligro de contaminación, alto.



MITOS, ENGAÑOS Y MENTIRAS SOBRE LOS CARTUCHOS DE IMPRESORA

Hola soy victor Soy de Alcantarilla(Murcia) Soy webmaster, por si os interesa mi web es www.kazatron.cjb.net y tambien se algo de informatica y hacking aqui os cuento como los cartuchos de tinta llegan a ser una estafa, el dinero esta expresado en dolares y pesos.
Aqui relato la estafas y mentiras de los cartuchos de tinta.

Lectura: "Mitos, engaños y mentiras sobre los cartuchos de impresora"
El primer punto es que compraste una maquina en cuotas por un valor de 100 veces su valor sin darte cuenta.
Mira, compraste una Lexmark, Z365 o alguna de esas que cuestan 100 pesos CON UN CARTUCHO o $160 con dos cartuchos. Cada cartucho vale $90 el color y $80 el negro,LA MAQUINA DICE QUE IMPRIME COMO 1000 HOJAS, pero al 5% en baja calidad, o sea un cirulo de 2,5 centimetros de diametro por hoja en calidad Draft. Vas a imprimir 150 hojas normales a un costo de $160¡¡¡¡. ¡¿Que compramos? cada hoja te cuesta $1 el mismo precio que el locutorio. Así que durante la vida util de la impresora (3 años) la vas a pagar varias veces

EL VALOR DE CUALQUIER MAQUINA ES IGUAL AL VALOR DE DOS CARTUCHOS QUE LLEVA. Ejemplo: una OPTRA E 210 Laser cuesta $680, cada cartucho cuesta $340, pero solo lleva uno. Ahora entendiste? es como comprar un Mercedez Benz a mil dolares , pero solo podes cargar nafta MERCEDES BENZ a 1000 el litro. Asi que la campaña en contra del reciclado tiene un fundamento, hay mucha plata para las fabricas. La nueva EPSON es el mejor caso , cada cartucho Dura BRITE cuesta $27 pero no te dijeron que no imprime mas de 50 hojas y que generalmente se gastan todos juntos, ya que el color rojo por ejemplo lleva Ciam (azul) Magenta (fucsia) y amarillo, para que lo veas rojo, asi que en realidad cada 50 hojas son 120 pesos QUE OFERTON ¡¡Abri los ojos.

COMPRE UN CARTUCHO HP (15 /45 / 23/ 78 / 35/ 41) o un LEXMAR (todos) COMPATIBLE
Noooo, lo engañaron no hay compatibles de ninguno de los antes mencionados son sacados de la basura y vueltos a cargar, los ponen en una bonita cajita y te lo venden por $50 - $ 60

COMPRE UN LASER COMPATIBLE
Noooo , lo engañaron no hay compatibles de ningun LASER, son sacados de la basura y vueltos a cargar, los ponen en una bonita cajita y te lo venden por un tercio mas barato que el ORIGINAL. La tecnologia de un laser cuesta 60 millones de dolares y ni para los chinos es negocio (las impresoras cambian rapidamente para evitar eso)

YO COMPRE UN EPSON COMPATIBLE Y ANDA BIEN.
Sí pero solo imprimen en calidad alta o media en DRAFT (baja) imprimen con rayas y tampoco te dijeron que PERDISTE LA GARANTIA de tu impresora ya que epson no acepta cartuchos compatibles y los podrias reciclar por alguien que sepa y te los deja como nuevos. Y la la notica mala es que al tercer cartucho que uses vas a tener que llevar tu maquina a la garantia, la tinta de los compatibles termina tapando los cabezales. Si los recargas tenes menos problemas y tenes tu cartucho original

LOS CARTUCHOS RECARGADOS DURAN MENOS
No es verdad, son trasparentes (los HP) y se ve la tinta en el caso de las EPSON el contador que tienen pertenece a la maquina, no tienen un bichito verde que sabe cuanta humedad hay dentro de un cartucho, SOLO cuentan la cantidad de copias que la impresora hace, sin importar si el cartucho es reciclado, nuevo o lo que sea.

EL CARTUCHO ME ARRUINO LA MAQUINA
Esta es la frase dicha por un neofito (alguien nuevo en un tema) se lo dijo el del service. La realidad es que lo mas que puede suceder es que manche con tinta la maquina, algo sin duda desagradable pero eso no le hace absolutamente nada a la maquina. En el caso de un EPSON puede suceder que si la tinta es mala se tape la impresora.

TE COMPRO EL CARTUCHO
Un señor muy dormido que pierde plata, le estan dando $10 por un cartucho que se puede recargar,es justamente por eso que se lo compran. Despues este mismo señor vuelve a comprarlo en ´´cajita´´ por $50 -$60 como ´´NUEVO El primer punto es que compraste una maquina en cuotas por un valor de 100 veces su valor sin darte cuenta.

COMPRE UN CARTUCHO NUEVO COREANO POR $ 70
Le engañaron, en todos los kioscos sale $ 55

COMPRE UN CARTUCHO HP NUEVO EN CAJITA Y DURO POCO
Es que la gente no sabe que ahora HP vende cartuchos con las letras ´´N´´o ´´D´´ que significa media carga y un tercio de carga, es el nuevo engaño de HP. Los cartuchos con letra ´´A´´ son full.

NO TE DEJES ESTAFAR, AL FINAL EL RECICLADO ES LO MEJOR PERO AVERIGUA LA MARCA DE RESPALDO QUE TENGAN, FIJATE SI TIENEN GARANTIA, QUE TE DEVUELVAN LA PLATA (LOS CARTUCHOS NO SON ETERNOS) AHI SI COMPRA NUEVOS..

VICTOR

¡Menudo caudal de información sobre diversos infundios relacionados con la tinta de impresora! Gracias por tu información. No podemos verificar todos y cada uno de los puntos que relatas, pero en cualquier caso es importante insistir en el tema. ¿Cómo se explica, si no, que prácticamente regalen muchos modelos de impresora? Obviamente, el negocio se ha deslizado hacia los consumibles, que es donde nos están esperando para recibir el óbolo...

¡HOT!

RETRASADA LA PRESENTACIÓN DE NUEVOS MOTOROLA

Motorola no presentó sus esperados teléfonos diseñados para trabajar con el servicio de música digital iTunes, de Apple Computer, en la feria Cebit celebrada en Alemania, ya que ambas empresas difieren en la forma de presentar los nuevos productos, dijeron ejecutivos de Motorola.

Motorola explicó que tiene la costumbre de presentar sus productos antes de que estén disponibles en el mercado pero que el jefe ejecutivo de Apple, Steve Jobs, defendía la postura de su compañía de presentarlos después.

"La perspectiva de Steve es que lancemos un producto el domingo y lo vendamos el lunes", añadió.

Motorola ha establecido la fecha de lanzamiento para los dos modelos de teléfonos móviles que pueden descargar música del servicio de iTunes para este año, presentado uno en la primera mitad de año y otro en la segunda.

ADIÓS A MOZILLA SUITE

Se comenta que la línea 1.7.x de lanzamientos será la última fase de desarrollo en cuanto a versiones nuevas del navegador desarrolladas por Mozilla. La 1.8 ya no se desarrollará, por lo menos por la fundación. Por supuesto si alguien de la comunidad open source está dispuesto a desarrollar el navegador no habrá nada que se lo impida.

De cualquier modo la Fundación ha expresado su deseo de centrar sus esfuerzos en dos productos: Mozilla Firefox como navegador y Mozilla Thunderbird como cliente de correo. Para los usuarios de la Suite Mozilla, denominada SeaMonkey, y que incluía navegador, cliente de correo y una herramienta de edición html, son malas noticias. Pero todos sabemos que los negocios son los negocios.

Esperemos que este hecho no frene el desarrollo de los navegadores libres sino que haga mas fuerte su expansión. Para un internet libre, una navegación libre.

http://www.mozilla.org

KERNEL 2.6, VULNERABLE

Se han descubierto diversas vulnerabilidades en la rama 2.6 del kernel de linux. Una tendría un impacto desconocido, mientras que las otras pueden ser explotadas para provocar denegaciones de servicio o comprometer un sistema afectado.

Una es un error en ROSE debido a la falta de verificación del argumento ndigis de nuevas rutas. Otro problema es que cualquier usuario con permisos de acceso a un dispositivo de cinta SCSI puede enviar algunos comandos que lo dejarían inoperativo para otros usuarios.

Finalmente, algunos errores sin especificar se han detectado en el procesador del sistema de archivos ISO9660, incluyendo las extensiones Rock Ridge y Juliet. Esto puede ser explotado por un sistema especialmente modificado para provocar una denegación de servicio o corromper la memoria para incluso ejecutar código arbitrario.

De todas formas todas las vulnerabilidades anteriormente citadas han sido resueltas con la velocidad a que nos tienen acostumbrados y ya se pueden descargar nuevos fuentes desde la página oficial. También podeis consultar el changelog de la nueva versión.

http://kernel.org/pub/linux/kernel/v2.6/testing/ChangeLog-2.6.12-rc1
http://www.kernel.org

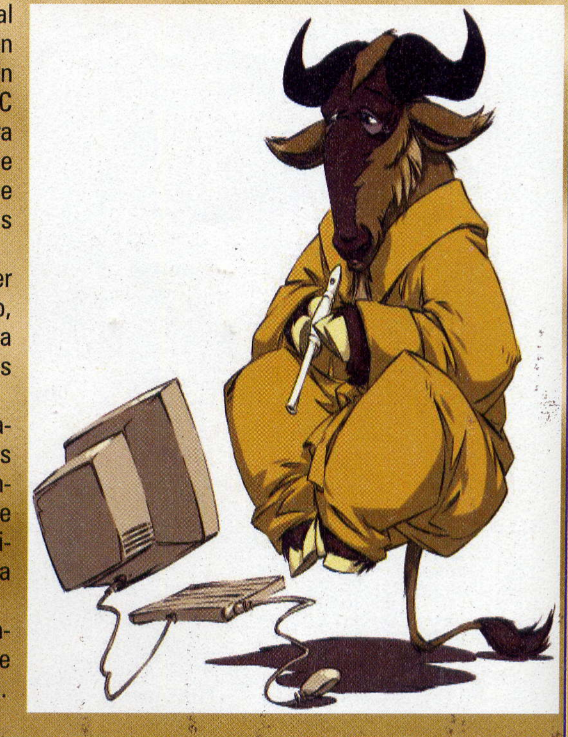
EL MIT RECOMIENDA SOFTWARE LIBRE A BRASIL

Recientemente Microsoft ofreció al gobierno de Brasil una versión simplificada de Windows de Microsoft en un nuevo proyecto denominado PC Conectado. El plan está diseñado para vender este año hasta un millón de ordenadores, con costes parcialmente subsidiados por el Gobierno, a brasileños con ingresos bajos o medios.

En una carta al Gobierno brasileño, Walter Bender, director de Media Lab del MIT dijo, "Aconsejamos usar software libre de alta calidad como contraposición a versiones sencillas de software más costoso".

La decisión final sobre qué software instalar se ha retrasado varias veces. Algunos miembros del gabinete creen que los consumidores deben tener elección entre comprar un ordenador con software gratuito o pagar un poco más por una máquina con software de Microsoft.

Sin embargo, defensores del software gratuito dentro del Gobierno de Lula creen que Microsoft debe ser excluido del programa.



➲ ENVÍOS MASIVOS DE E-MAILS FRAUDULENTOS

La AUI (Associación de Usuarios de Internet) alertó hace poco del notable incremento de e-mails fraudulentos que solicitan datos personales y claves de acceso a servicios bancarios.
Estos correos, que simulan en su presentación las páginas de banca electrónica de diferentes entidades, tienen por objetivo el robo de datos que son facilitados para rellenar un formulario en el que se piden las claves de acceso, que en lugar de ir al banco son enviadas a los autores de la estafa.
Esta práctica, denominada 'phising' ha sido puesta en práctica en las últimas horas con falsos servicios de atención al cliente de las entidades BBVA y Cajamadrid. La Asociación de Internautas pidió hoy en un comunicado a las distintas entidades financieras objeto de estos fraudes que informe a sus clientes de estas actuaciones delictivas, para que tengan información adecuada y no se de ningún tipo de duda al respecto.
Internet cada vez más nuestra gran selva binaria (con sus depredadores).

➲ CONSOLIDACIÓN DEL CABLE EN EUROPA

La consolidación del sector del cable en Europa continuará en 2005 y en años posteriores y resultará "vital" para el impulso del sector, según se desprende del estudio realizado por la consultora Ovium para la Asociación de Comunicación del Cable Europeo (ECCA) y presentado en su 51º Congreso Anual, que se celebra en Budapest.
El informe resalta que la consolidación del sector "forma parte de un proceso necesario para garantizar el tamaño necesario para el desarrollo sostenible del negocio y que, de esta forma, las compañías de cable europeas puedan continuar ofreciendo a los consumidores la más amplia variedad de servicios con la máxima calidad".
Según han manifestado los máximos responsables de ambas compañías en múltiples ocasiones, la fusión de Ono y Auna está destinada a producirse en algún momento. La principal duda es si se articulará mediante la compra de una compañía por otra o será una fusión entre iguales mediante un canje de acciones.
El estudio indica asimismo que en las regiones donde se comercializan servicios de "triple play" (teléfono, televisión e Internet) de cable la penetración de Internet de banda ancha es hasta tres veces superior a la del resto de regiones, y además el servicio telefónico es más barato.
El crecimiento del sector se verá impulsado por los servicios de Internet y telefonía y la puesta en marcha de los servicios de televisión digital y del vídeo bajo demanda potencian el atractivo de la oferta de "triple play" de cable, a pesar de la competencia de las operadoras tradicionales o de las redes digitales terrestres.



Este hecho podria beneficiar el abandono de tecnologías menos evolucionadas como ADSL y sus derivados de cobre. Abrir las puertas a la fibra óptica, a la banda ancha.



➲ GOOGLE CODE

Y otra vez más google vuelve a estar dentro de nuestra sección de noticias. Esta vez la empresa americana ha lanzado un site para aumentar las relaciones con los desarrolladores de software ofreciendo código libre.
El nuevo site, llamado Google code ha estado en desarrollo durante seis meses y aunque la compañía ha reconocido sus modestos inicios, espera que aumente su alcance.
El site tiene como objetivo ofrecer a la comunidad de fuente abierta herramientas de software desarrolladas y utilizadas internamente por Google, aportando código que los desarrolladores externos podrían encontrar útil.
Aunque Google Code incluye enlaces a información de los interfaces de programación de aplicaciones (APIs) de Google, el objetivo del site, según la compañía, no es conseguir que los desarrolladores externos escriban aplicaciones para aumentar la funcionalidad de Google, que cuenta con un site diferente para sus APIs.

http://code.google.com/

➲ HACKERS VS. MACOS X

La compañía de software de seguridad Symantec ha dado la alerta porque Mac O SX comienza a ser objetivo de los hackers. Los profesionales de la seguridad detectaron el año pasado 37 vulnerabilidades en Mac OS X. De acuerdo con Symantec, Apple está aumentando su cuota de mercado, con nuevos productos de bajo coste como el Mac mini, lo que puede aumentar la cantidad de ataques.
"Contrariamente a lo que creen muchos el sistema operativo de Macintosh, no es completamente invulnerable al código malicioso" comentó Symantec. "Fuera del gran público durante algún tiempo, ahora se puede ver claramente que Mac OS X es un objetivo potencial para los hackers."
Esperemos que este SO basado en unix sepa aguantar firme la popularización cada vez más evidente que esta consiguiendo (otra vez) el señor Jobs.

FUERA BARRERAS A LA VÍDEO

Para hablar y verse de modo seguro entre usuarios de NetMeeting a través de firewall lo mejor es pasar de NetMeeting

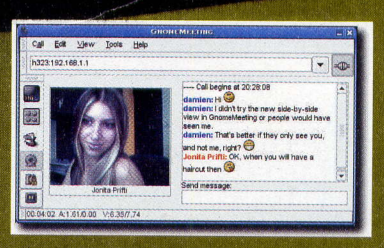
NetMeeting es un programa de videoconferencia muy difundido y mucha gente se lamenta de problemas para alcanzar tal o cual contacto. Bien: es culpa de un firewall que, en nuestra parte o en la del otro, no quiere abrir los puertos necesarios. Pero también es culpa de NetMeeting, que es un programa desastrosamente inseguro.

Puertos abiertos

Según Microsoft, para pasar a través de un firewall con Netmeeting, los puertos a abrir son los siguientes:

Puerto 389
Internet Locator Server (Transmission Control Protocol, TCP)
Puerto 522
User Location Server (TCP)
Puerto 1503
T.120 (TCP)
Puerto 1720
H.323 call setup (TCP)
Puerto 1731
Audio call control (TCP)

Parece acabar aquí, pero no es cierto. NetMeeting pide también la apertura de conexiones UDP (User Datagram Protocol) asignadas dinámicamente a puertos comprendidos en el intervalo 1024-65535. ¡Prácticamente NetMeeting quiere abiertos todos los puertos del equipo! Entonces el firewall es inútil. Al estilo Microsoft. Y he aquí por qué típicamente NetMeeting se usa mucho en las redes locales y menos en Internet. No es el caso de una conexión a una dirección IP, pero si quisiéramos usar los servicios de directorio de NetMeeting tendríamos que usar también el puerto 389 (NetMeeting 2 y siguientes) o el puerto 522 (NetMeeting 1.0).



GnomeMeeting es la solución open source a la videoconferencia. Funciona, en todos los equipos que existen.

Donde los routers implantados lo permiten, un compromiso posible es situar el PC en la DMZ del rou-



QUÉ ES UNA DMZ

El acrónimo significa Demilitarized Zone: un equipo o una subred que se encuentra en medio entre una red interna segura, por ejemplo una red privada, y una red externa no segura, como Internet. Típicamente una DMZ contiene equipos accesibles al tráfico de Internet, como servidores Web y FTP. El término proviene de la jerga militar, e indica una tierra de nadie entre dos despliegues enemigos.



CÓMO EMPIEZA UNA VIDEOCONFERENCIA NETMEETING

El protocolo de configuración de llamada (call setup protocol) H.323 negocia dinámicamente por el puerto 1720 la apertura de un puerto TCP a usar por parte del control de llamada de H.323. El mismo call setup protocol y el control de la parte de audio (audio call control protocol, éste por el puerto 1731) negocian dinámicamente los puertos UDP a usar para el protocolo de streaming de H.323, llamado Real Time Procotol (RTP). En NetMeeting, en cada lado del firewall se negocian dinámicamente dos puertos, para el streaming de audio y vídeo. Los puertos se asignan arbitrariamente entre los disponibles.

CONFERENCIA

↑ *También iVisit es mejor que NetMeeting, con una compatibilidad superior. ¡El sevicio básico es gratuito!*

ter. No hay seguridad total y estará más seguro sacar el PC de la DMZ en cuanto termine la conexión. Pero es mejor que nada.

Si las conexiones de vídeo se dan a menudo, tal vez sea oportuno empezar a considerar el uso de un programa distinto de NetMeeting, que será menos imprudente al abrir puertos y probablemente será también un poco más simple de usar.

QUÉ ES UN USER DATAGRAM PROTOCOL

Abreviado como UDP, es un protocolo de comunicación que funciona en redes IP (Internet, vamos). A diferencia de TCP/IP, UDP/IP está mucho menos atento a la precisión de los datos. Pero precisamente por ello es más veloz y adaptado para transmitir datos como audio y vídeo.

Alternativas

Hay decenas de buenos programas para hacer videoconferencia, desde Yahoo Messenger, que es una elección poco funcional, hasta PalTalk, que podemos encontrar en http://www.paltalk.com/PalTalkSite/index.html. Otra alternativa es IVisit, http://www.ivisit.com/, que tiene la ventaja de estar también en versión Macintosh. Para los aventureros se recomienda GnomeMeeting (http://www.gnomemeeting.org/), que funciona bien en Linux y Unix, tiene una versión para Windows y funciona con un poco de trabajo también en Mac.

Pero las opciones son muchísimas y, por poner sólo un ejemplo, en VersionTracker (http://www.versiontracker.com) las hay a montones.

¡Ahora ya sabemos qué hacer!

El 3D de las FIRMAS

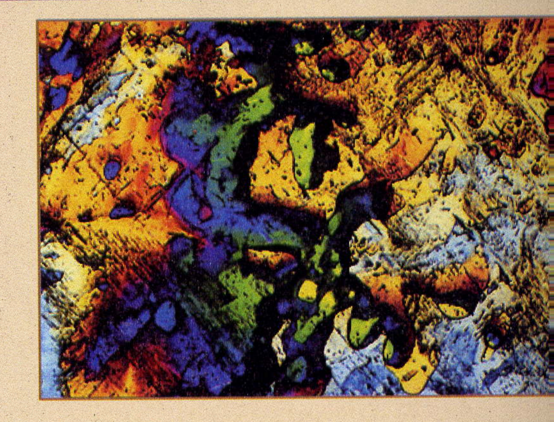
Tiempos dificiles para los falsificadores; el antiguo arte de la miniatura ya no bastará para falsificar la firma de cuentas, tarjetas de crédito y documentos. La reproducción del perfil 3D de una firma quedará reservado a pocos y buscadísimos expertos.





En la perenne guerra entre policías y ladrones, la tecnología puede asestar un duro golpe a los falsificadores y en particular a los imitadores de caligrafías, quienes crackean cuentas y tarjetas de crédito. Se puede ver en los seriales televisivos más banales que las hojas inferiores a aquella en la que la víctima (o el asesino) han escrito algo conservan la huella del mensaje, porque el escrito no es sólo bidimensional como un trazo, sino en tres dimensiones. Quien escribe hace presión sobre el papel, y deja una huella de cierta profundidad, mínima pero mensurable. La más obvio es que esta profundidad es personal y varía con cada persona. Pero lo menos obvio es la posibilidad de reconocer la caligrafía y detectar las falsificaciones en base a la huella tridimensional del mensaje.

Las tecnologías más avanzadas permitirán derrotar para siempre toda una categoría de farsantes: los de las FIRMAS AJENAS

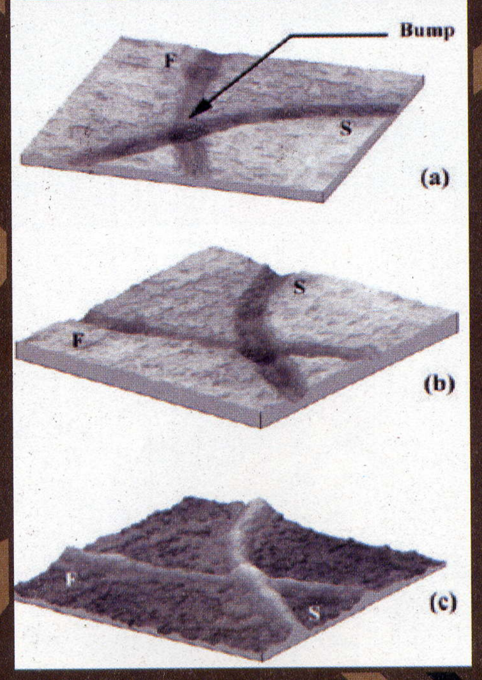


Señoras y señores, la microperfilometría

La nueva técnica se denomina microperfilometría 3D y trabajan en ella investigadores de la universidad italiana de Roma Tres. Según ellos puede ser una función decisiva en la lucha contra los falsificadores. El primer paso consiste en realizar un modelo tridimensional de la presión aplicada durante la escritura del texto.

La firma en tres dimensiones proporciona información clara, respecto a la sola huella de tinta, de la superposición y dirección de los trazos de la pluma. Estos elementos se usan habitualmente en el reconocimiento convencional de la caligrafía, pero a menudo son confusos o no se pueden reconstruir sin la indicación decisiva de la tercera dimensión.

En el modelo 3D son visibles las depresiones y las crestas creadas durante el escrito, y es simple reconstruir la formación de la firma, dejando intacto el trazo original, cosa que las técnicas actuales no siempre garantizan. A menudo es imposible disponer del poseedor legítimo de la firma (por ejemplo en las disposiciones testamentarias) y por ello conservar la integridad del escrito.



El material utilizado para recuperar el rastro 3D de la escritura a mano. Ingredientes principales, láser y módulo conoscópico.

Adiós calco

Los falsificadores de escritura siempre han sabido calcar las firmas, pero ultimamente han empezado a utilizar también métodos evolucionados de copia a mano alzada. Pero, con la tercera dimensión, su misión pronto se hace imposible. El falsificador tiene típicamente poco tiempo y pocos recursos. En estas condiciones, es difícil que logren reproducir un perfil 3D de una firma.

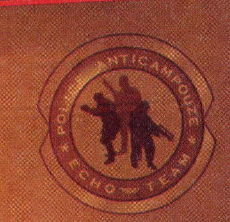
Al perito caligráfico de la policía, por el contrario, pueden bastar un par de horas de análisis para producir un resultado incontestable y libre de ambigüedades.

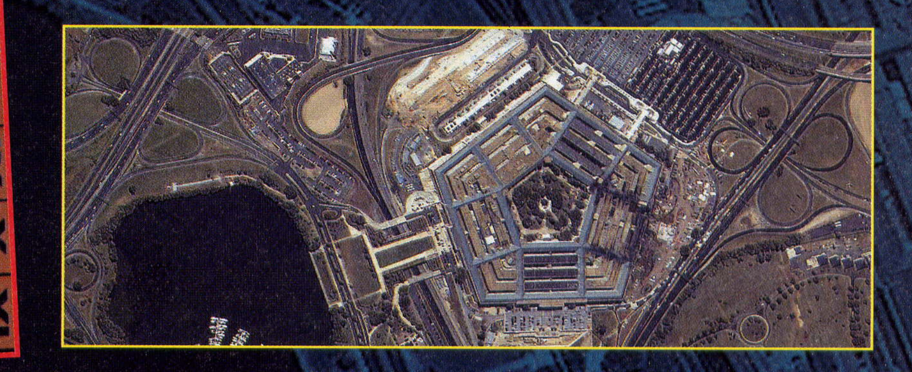
Las primeras aplicaciones de la microperfilmetría 3D parecen bastante prometedoras. El porcentaje de reconocimiento correcto supera en efecto ya el 90 por ciento, sobre una recopilación experimental de 126 cartas escritas por otros tantos autores diferentes, que incluye ciertamente los previsibles bolígrafos pero también estilográficas y rotuladores, sobre soportes que van desde el papel común hasta los cheques pasando por el cartón prensado.

La escritura con bolígrafo sobre papel común es la combinación más fácil, donde el reconocimiento pasa con certeza prácticamente absoluta. En fin: en el futuro el robo de la tarjeta de crédito y otros problemas semejantes causarán menos daños, gracias a la firma tridimensional que dejamos sin saberlo cuando escribimos en las dos dimensiones de la hoja de papel.

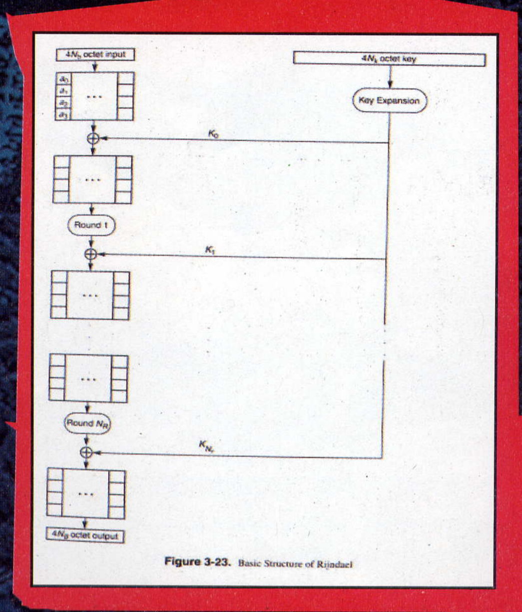
Seguros con AES

El algoritmo de cifrado de documentos top secret del gobierno de EE.UU.





El Advanced Encryption Standard, también conocido como Rijndael, es el sucesor de DES como algoritmo de cifrado estándar para el gobierno de EE.UU. Fue seleccionado en noviembre de 2001 tras cinco años de puesta a punto. El nombre de Rijndael (se pronuncia como RAINdal o bien como RAINdau) recuerda en una sola palabra a Joan Daemen y Vincent Rijmen, los dos criptógrafos belgas que presentaron el algoritmo, evolución de un primer esquema de nombre Square, a su vez desarrollado por Shark.
Rijndael es una red de sustitución-permutación, muy veloz tanto por software como por hardware, relativamente fácil de programar y poco exigente de memoria. En rigor Rijndael y AES no son técnicamente lo mismo: el segundo tiene un tamaño de bloque fijo a 128 bits y claves de 128, 192 o 256 bits, y el primero tiene bloque y claves de tamaño variable múltiplo de 32 bits entre un mínimo de 128 y un máximo de 256 bits. Pero en la práctica son intercambiables y por tanto hablaremos sólo de AES para englobar ambos.



← La estructura básica de AES, o Rijndael. La pieza fundamental es una matriz de 4 x 4 bytes.

right (low-order) nibble

left (high-order) nibble	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 3-24. Rijndael S-box

↑ *La S-box es una tabla de sustitución que se aplica a la matriz como primera operación de cifrado. Las cifras hexadecimales se han elegido con cuidado para no dar pistas matemáticas al descifrado.*

Algoritmo de estado

AES trabaja sobre una matriz de 4 x 4 bytes llamada estado. Cada ciclo de cifrado, excepto el último, está compuesto por cuatro fases: SubBytes, ShiftRows, MixColumns y AddRoundKey. En el último ciclo salta MixColumns.

SubBytes actualiza cada byte en la matriz usando una S-box de ocho bits. La S-box se crea con propiedad de no linealidad y de modo que no tenga puntos fijos, fáciles de atacar.

ShiftRows trabaja sobre las líneas de la matriz, desplazándolas un cierto valor (el offset). La primera línea no cambia; cada byte de la segunda se desplaza un lugar a la izquierda; los bytes de la tercera y cuarta línea se desplazan a la izquierda dos y tres lugares respectivamente. Así, cada columna de salida contiene elementos provenientes de cada columna de entrada.

MixColumns toma los cuatro bytes de cada columna y los combina mediante una transformación lineal invertible, procediendo a una ulterior elaboración para aumentar sus características de difusión. AddRoundKey combina matriz y subclave. Ésta, derivada de la clave y del propio tamaño de la matriz, se somete a XOR con la matriz. A cada byte de la matriz le corresponde el byte equivalente de la subclave.

right (low-order) nibble

left (high-order) nibble	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00	02	04	06	08	0a	0c	0e	10	12	14	16	18	1a	1c	1e
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
	00	03	06	05	0c	0f	0a	09	18	1b	1e	1d	14	17	12	11
1	20	22	24	26	28	2a	2c	2e	30	32	34	36	38	3a	3c	3e
	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
	30	33	36	35	3c	3f	3a	39	28	2b	2e	2d	24	27	22	21
2	40	42	44	46	48	4a	4c	4e	50	52	54	56	58	5a	5c	5e
	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
	20	21	22	23	24	25	26	27	28	29	2a	2b	2c	2d	2e	2f
	60	63	66	65	6c	6f	6a	69	78	7b	7e	7d	74	77	72	71
3	60	62	64	66	68	6a	6c	6e	70	72	74	76	78	7a	7c	7e
	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
	30	31	32	33	34	35	36	37	38	39	3a	3b	3c	3d	3e	3f
	50	53	56	55	5c	5f	5a	59	48	4b	4e	4d	44	47	42	41
4	80	82	84	86	88	8a	8c	8e	90	92	94	96	98	9a	9c	9e
	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
	40	41	42	43	44	45	46	47	48	49	4a	4b	4c	4d	4e	4f
	c0	c3	c6	c5	cc	cf	ca	c9	d8	db	de	dd	d4	d7	d2	d1
5	a0	a2	a4	a6	a8	aa	ac	ae	b0	b2	b4	b6	b8	ba	bc	be
	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
	50	51	52	53	54	55	56	57	58	59	5a	5b	5c	5d	5e	5f
	f0	f3	f6	f5	fc	ff	fa	f9	e8	eb	ee	ed	e4	e7	e2	e1
6	c0	c2	c4	c6	c8	ca	cc	ce	d0	d2	d4	d6	d8	da	dc	de
	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
	60	61	62	63	64	65	66	67	68	69	6a	6b	6c	6d	6e	6f
	a0	a3	a6	a5	ac	af	aa	a9	b8	bb	be	bd	b4	b7	b2	b1
7	e0	e2	e4	e6	e8	ea	ec	ee	f0	f2	f4	f6	f8	fa	fc	fe
	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f
	70	71	72	73	74	75	76	77	78	79	7a	7b	7c	7d	7e	7f
	90	93	96	95	9c	9f	9a	99	88	8b	8e	8d	84	87	82	81
8	1b	19	1f	1d	13	11	17	15	0b	09	0f	0d	03	01	07	05
	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f
	80	81	82	83	84	85	86	87	88	89	8a	8b	8c	8d	8e	8f
	9b	98	9d	9e	97	94	91	92	83	80	85	86	8f	8c	89	8a
9	3b	39	3f	3d	33	31	37	35	2b	29	2f	2d	23	21	27	25
	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f
	90	91	92	93	94	95	96	97	98	99	9a	9b	9c	9d	9e	9f
	ab	a8	ad	ae	a7	a4	a1	a2	b3	b0	b5	b6	bf	bc	b9	ba
a	5b	59	5f	5d	53	51	57	55	4b	49	4f	4d	43	41	47	45
	a0	a1	a2	a3	a4	a5	a6	a7	a8	a9	aa	ab	ac	ad	ae	af
	a0	a1	a2	a3	a4	a5	a6	a7	a8	a9	aa	ab	ac	ad	ae	af
	fb	f8	fd	fe	f7	f4	f1	f2	e3	e0	e5	e6	ef	ec	e9	ea
b	7b	79	7f	7d	73	71	77	75	6b	69	6f	6d	63	61	67	65
	b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	ba	bb	bc	bd	be	bf
	b0	b1	b2	b3	b4	b5	b6	b7	b8	b9	ba	bb	bc	bd	be	bf
	cb	c8	cd	ce	c7	c4	c1	c2	d3	d0	d5	d6	df	dc	d9	da
c	9b	99	9f	9d	93	91	97	95	8b	89	8f	8d	83	81	87	85
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	ca	cb	cc	cd	ce	cf
	c0	c1	c2	c3	c4	c5	c6	c7	c8	c9	ca	cb	cc	cd	ce	cf
	5b	58	5d	5e	57	54	51	52	43	40	45	46	4f	4c	49	4a
d	bb	b9	bf	bd	b3	b1	b7	b5	ab	a9	af	ad	a3	a1	a7	a5
	d0	d1	d2	d3	d4	d5	d6	d7	d8	d9	da	db	dc	dd	de	df
	d0	d1	d2	d3	d4	d5	d6	d7	d8	d9	da	db	dc	dd	de	df
	6b	68	6d	6e	67	64	61	62	73	70	75	76	7f	7c	79	7a
e	db	d9	df	dd	d3	d1	d7	d5	cb	c9	cf	cd	c3	c1	c7	c5
	e0	e1	e2	e3	e4	e5	e6	e7	e8	e9	ea	eb	ec	ed	ee	ef
	e0	e1	e2	e3	e4	e5	e6	e7	e8	e9	ea	eb	ec	ed	ee	ef
	3b	38	3d	3e	37	34	31	32	23	20	25	26	2f	2c	29	2a
f	fb	f9	ff	fd	f3	f1	f7	f5	eb	e9	ef	ed	e3	e1	e7	e5
	f0	f1	f2	f3	f4	f5	f6	f7	f8	f9	fa	fb	fc	fd	fe	ff
	f0	f1	f2	f3	f4	f5	f6	f7	f8	f9	fa	fb	fc	fd	fe	ff
	0b	08	0d	0e	07	04	01	02	13	10	15	16	1f	1c	19	1a

↑ *Esta tabla de referencia se aplica a la operación MixColumns.*

Seguro, por ahora

Hasta hoy no se han encontrado ataques resolutivos contra AES. El gobierno americano permite su uso para la información confidencial especificando una clave mínima de 128 bits para los documentos SECRET y de 192 o 256 bits para los TOP SECRET. Siendo el algoritmo de dominio público, es la primera vez en la historia que cualquiera puede tener acceso al sistema de cifrado usado en documentos top secret.

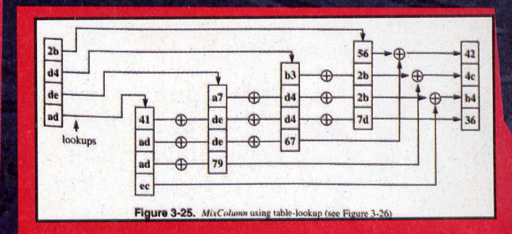


Figure 3-25. MixColumn using table-lookup (see Figure 3-26)

↑ *Esquema de funcionamiento de la tabla MixColumns.*

La información top secret relativa a los hechos del 11 de septiembre de 2004 está cifrada en AES.

No durará siempre; por ejemplo, en 2002 Nicolas Courtois y Josef Pieprzyk mostraron una una debilidad potencial en el algoritmo, que algún día puede hacer viable un ataque, hoy fuera de alcance. Pero AES, o Rijndael, representa en estos momentos una de las mejores opciones posibles para proteger nuestros datos. La definición oficial y completa del algoritmo se encuentra en http://csrc.nist. gov/publications/fips/ fips197/fips-197.pdf. El código fuente está en http://www.cr0.net:8040/code/crypto/aes/.

PS2, NO TOCAR

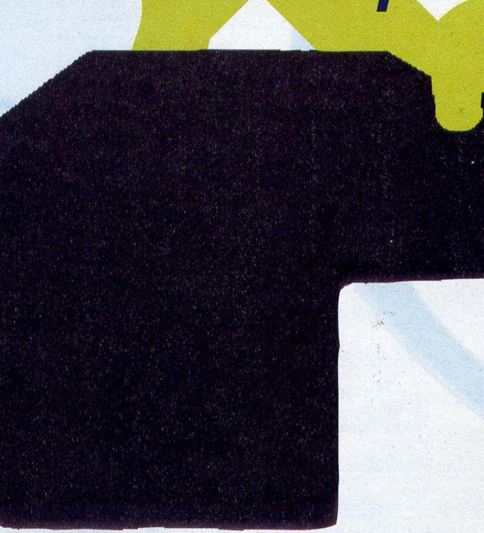
Con la slide card, los flip top y la neo key ya no es preciso tocar los chips

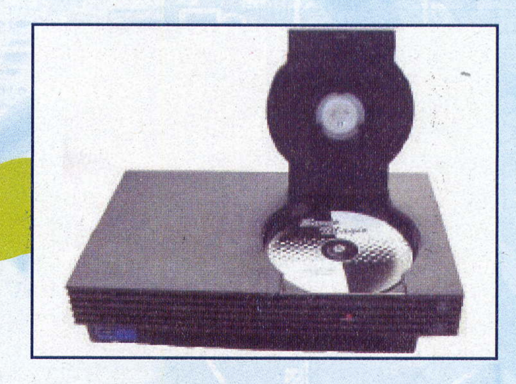
Al principio eran los mod-chip. Se cambiaban los chips de la PlayStation -o de cualquier otra cosa- para obtener un resultado no previsto por el constructor o rodear una limitación. Un cambio de chip típico se hace para permitir que la PlayStation lea juegos provenientes de otras regiones geográficas, o bien para leer los backups de nuestros juegos.

Slide,... ¡NO CHIP!

No cambian internamente el sistema. Actúan cuando es necesario y la PlayStation queda exactamente como era al principio cuando ya no se necesita. En la práctica no son más que un sistema para abrir el lector de CD sin que la consola lo sepa.

La Slide card es un pequeño instrumento de plástico para extraer mecánicamente la bandeja; es el sistema más económico pero requiere una pequeña intervención técnica: desmontar el frontal del lector de DVD de





la PlayStation (basta con un destornillador).

Es un poco más fácil proceder con un Flip Top, una carcasa para PlayStation dotada de apertura de la bandeja de CD/DVD en la cara superior, que sustituye la carcasa original.

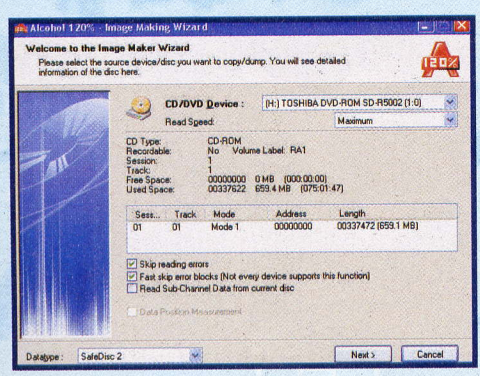


Nuevos modos fáciles, originales e indoloros para ampliar la capacidad de nuestra consola

EL CHIP

La Neo Key en cambio es lo mejor: es un módulo que, una vez insertado en uno de los puertos USB de la PlayStation, funciona automáticamente.

Sea cual sea la solución de hardware elegida, se requiere algo que funcione como disco de arranque. Uno de los sistemas es el disco Swap Magic. Se inserta el disco Swap Magic como si fuera un juego cualquiera. Cuando vemos la solicitud de insertar un disco, se abre el lector, se inserta el CD de importación o de backup y se cierra el lector, para luego pulsar x en el mando. La operación descrita es imposible, en una PlayStation sin modificaciones. En cambio, la combinación del software (Swap Magic) y de uno a elegir entre los dispositivos (Slide card, Neo Key o Flip Top) permite iniciar el juego, la sustitución del disco y la continuación, como si hubiera ocurrido nada.



↑ El mejor programa para preparar las copias de seguridad de nuestros discos de PlayStation 2. http://www-alcohol-soft.com.

EN LA TIENDA O EN LA RED

Una slide card se puede comprar en nuestra tienda de videojuegos habitual, si es un buen vendedor. Si no es así, se puede pedir por Internet sin problemas. Una de tantas direcciones posibles donde se puede encontrar: http://www.modchipstore.com/customer/product.php?productid=16158.
Una de tantas posibles direcciones para la Neo Key: http://www.thegiantstore.com/index.asp?PageAction=VIEWPROD&ProdID=121.
Un Flip Top, siempre como ejemplo, se puede comprar online en http://www.ultimateconsoleguides.com/FlipTop.htm. Pero lo más práctico sigue siendo dirigirse a un buen vendedor.





SPAM: tiene los

STOP SPAM

FILTROS ANTISPAM NO DE SERIE

Práticamente todos los programas de correo instalados en nuestro sistema contienen filtros antispam. Pero hay más donde elegir. Veamos algunos:

WINDOWS
SpamBayes, freeware:
http://spambayes.sourceforge.net/

MAC OS X
Lockspam Free, freeware:
http://www.polesoft.com/lockspam.html

LINUX
Bogofilter, freeware:
http://freshmeat.net/projects/bogofilter

PARA TODOS
SpamTUNNEL, freeware:
http://uiorean.cluj.astral.ro



AÑOS CONTADOS

La guerra al Spam no conoce tregua, he aquí los filtros que por fin acabarán con la producción de correo basura

De la apertura de una dirección de correo a la llegada del primer mensaje no deseado pueden pasar unos minutos. En poco tiempo pueden llegar hasta decenas al día. Sin embargo hoy los mejores filtros interceptan hasta el 99% de la porquería que llega. Si todos usáramos un buen filtro, probablemente el spam ya estaría muerto. No es así, todavía; todo llegará. La primera generación de filtros antispam usaba reglas de reconocimiento elemental, a partir de la identificación del remitente, del asunto o de palabras clave presentes en el correo. Los nuevos filtros funcionan mejor, comparando con bases estadísticas todo el mensaje con los demás que llegan y declarando spam lo que se parece en gran medida al spam ya conocido. Si la palabra cash, por ejemplo, aparece en 200 spam de cada 1.000 y en 3 spam de cada 500, la probabilidad de que un nuevo mensaje que contenga cash sea basura equivale a

(200/1000) / (3/500 + 200/1000) = 0,971, o el 97,1%.

Los filtros de verdad hacen cálculos más complicados que éste, pero la base del razonamiento es la misma.

Filtros como setas

En los últimos años los filtros de este tipo han aparecido por docenas, como setas tras la lluvia, probablemente porque el spam ha sido reconocido por fin como un problema universal. Todos los grandes productores de software, Microsoft y Apple a la cabeza, tienen su filtro, y en el mundo del Open Source hay muchos.
Hay ligeras diferencias de funcionamiento. El ejemplo que hemos puesto antes puede ser el primer paso de un filtro bayesiano estúpido.
Los bayesianos estúpidos (inteligentes porque son bayesianos; estúpidos por su aproximación simplista, no porque trabajen mal) incluyen muchos filtros Open Source y el filtro de MSN, y probablemente también el de Apple.

Las ventajas de los filtros bayesianos

Son muy eficaces. Hasta los más simples llegan al 99% de precisión. El más exacto hoy, CRM114 de Bill Yerazunis, llega al 99,8%. Con pocos falsos positivos. Lo peor que puede ocurrir a veces es arrojar por error en el spam un mensaje verdadero e importante. Con estos filtros sucede de vez en cuando.
Aprenden. cash es un indicio de spam muy fuerte. Pero también modalities (presente en muchos spam que envían dinero desde Nigeria) y FF0000 (código HTML del rojo intenso). Los

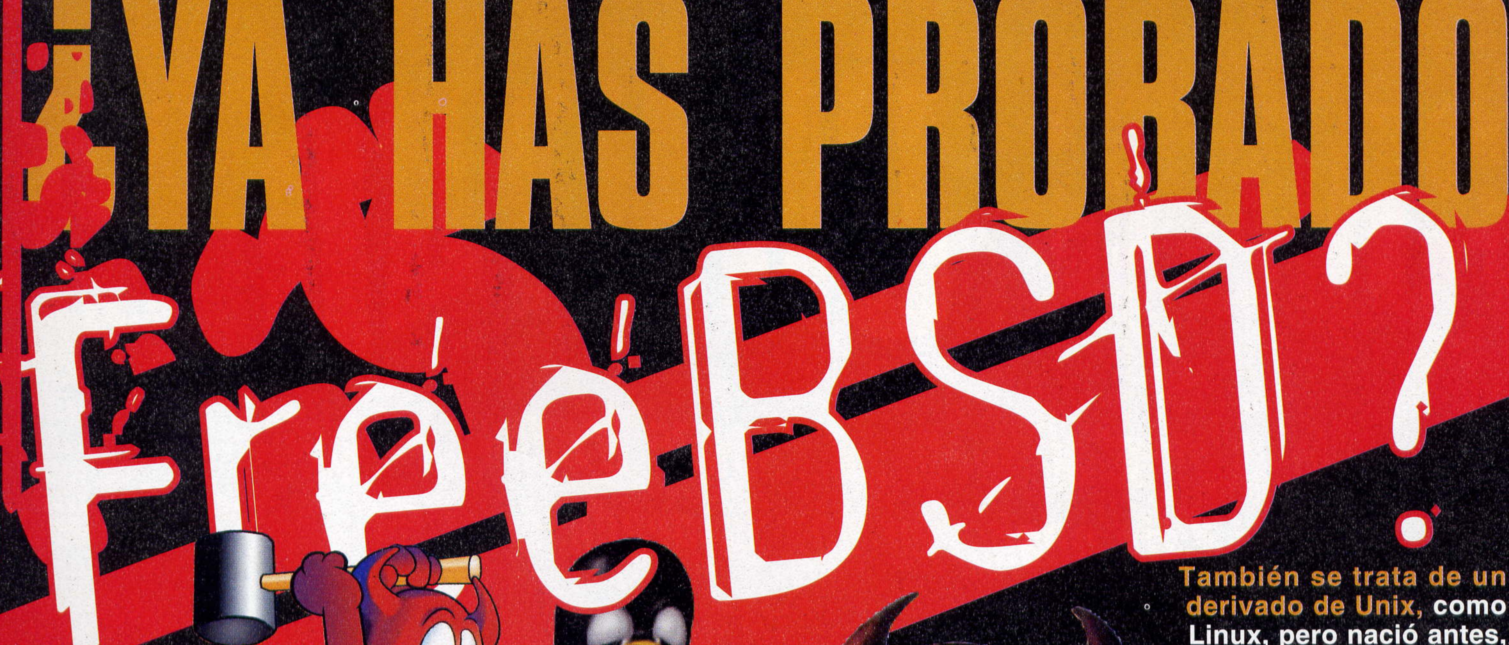


filtros aprenden a entender y se adaptan a los cambios de proceder de los spammer. Permiten definir manualmente el spam. Según nuestra experiencia, cosa importante. Són difíciles de engañar, sólo si usan pocas palabras o si usan palabras inocentes. La segunda opción, para el spammer, es difícil. La primera es compleja, porque los filtros aprenden también a reconocer palabras mal escritas, como peniss. Tienen que usar palabras cada vez más vagas, o texto escrito al azar, y poner un link, y esperar que cuele.

Engañar a los pardillos

Los filtros desechan el spam apenas llega, y esto es mucho. Pero ¿cómo derrotarlo? Es preciso que nadie responda al spam, o que sean tan pocos que lo hagan antieconómico. Por desgracia basta que respondan diez o quince pardillos, entre un millón de usuarios, para justificar la inversión en spam. Por ello el verdadero reto es insertar los filtros en los programas de modo que el spam ni siquiera llegue al incauto que quiera responder. Costará, pero lo conseguiremos.

¿YA HAS PROBADO FreeBSD?



El software libre es un universo en el que Linux es una galaxia importante. Pero hay muchas galaxias y una de las más interesantes es ésta

Muchos ni siquiera saben que existen magníficas alternativas al uso de Windows. Otros lo saben, pero piensan que existen sólo Macintosh y Linux. Noticia para todos: hay muchos sistemas operativos. Uno de los más interesantes, potente, seguro, libre y gratuito, es FreeBSD.

También se trata de un derivado de Unix, como Linux, pero nació antes, de una costilla del sistema BSD creado en California, en la universidad de Berkeley, cerca de San Francisco.

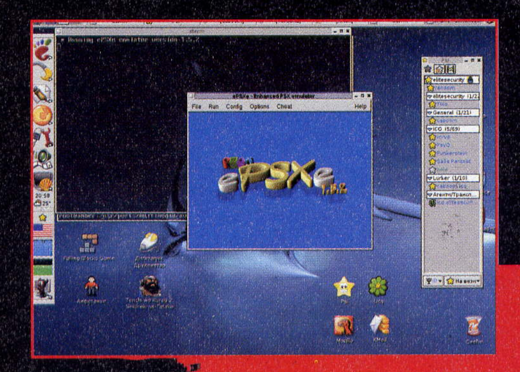
Funciona en todas partes

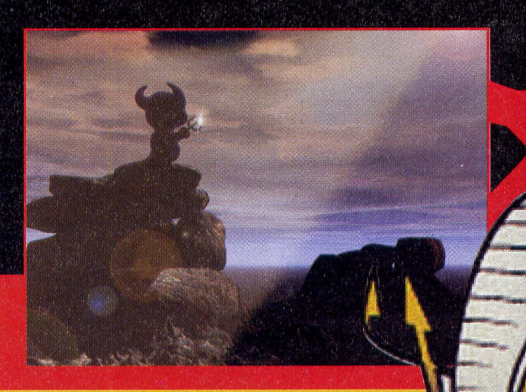
FreeBSD funciona prácticamente en cualquier procesador existente, Pentium, Athlon, AMD, Opteron, EM467, pero también el PowerPC del Macintosh y Alfa, Itanium, PC-98, UltraSPARC, MIPS y alguno más. No hay equipo producido en los últimos diez años que no pueda montar FreeBSD.

Cómo se usa

Al ser un sistema de tipo Unix, FreeBSD puede controlarse mediante

FreeBSD The Power to Serve www.FreeBSD.org







una interfaz gráfica o bien con comandos de texto desde un shell (prácticamente un editor de texto completo). Quien haya probado Mac OS X o Linux sabe de qué hablamos. También en Windows es posible hacer mucho con el prompt de comandos de MS-DOS, un entorno parecido.

¿Qué se puede hacer? De todo. Todos los programas famosos open source están disponibles en FreeBSD. OpenOffice puede leer todos los documentos creados con Office de Microsoft. Se puede navegar en el Web con Mozilla, leer el correo, cualquier cosa, con la interfaz gráfica que queramos, ya sea Gnome u otra.

Algún ejemplo de comando

Suponiendo que usamos el shell y no la interfaz gráfica, vemos ejemplos de comandos posibles. Seguimos la tradición Unix e indicamos con % lo que escribe un usuario normal: root es #.

%adduser
añade un nuevo usuario

% exit
ejecuta el logout

% id
indica la identidad, es decir, quién somos en el sistema

% pwd
muestra el directorio de trabajo actual

% ls
lista los archivos en el directorio actual

% cat
muestra el contenido de un archivo en la pantalla

% apropos
consulta la base de datos whatis y dice qué ordenes ejecutan una cierta función

% rm
borra un archivo

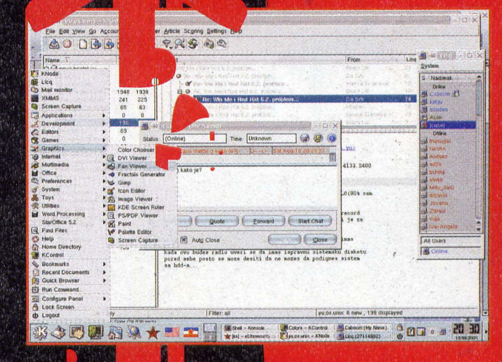
Quien conozca Linux o Mac OS X advertirá que las diferencias son mínimas o nulas.

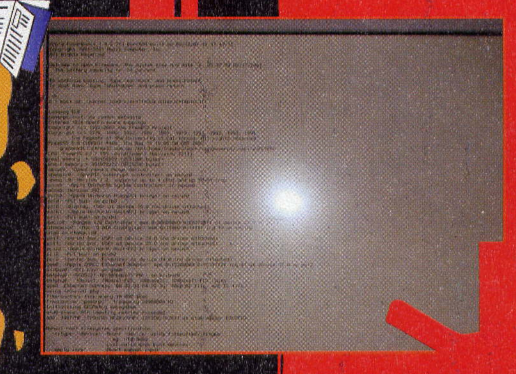
Pero entonces, dirá alguien, ¿por qué no usar Linux o Mac OS X? Porque la diversidad beneficia a la evolución, y FreeBSD monta un motor interno (el kernel) bastante diferente de Linux. Ello lo hace, por ejemplo, algo más seguro. Además, saber usar más sistemas operativos es como saber más idiomas: ¡entrena al cerebro y para hackers como nosotros es esencial!

Volveremos a hablar de FreeBSD con mayor detalle. ¡Quien esté interesado que empiece a experimentar!



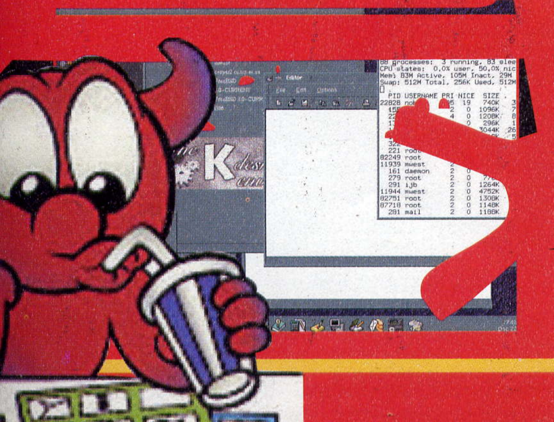




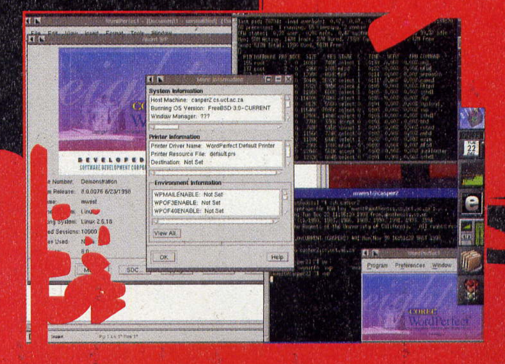


LO ESENCIAL DE FREEBSD

El sitio de referencia de FreeBSD es obviamente http://www.freebsd.org (¡disponible en español!), donde se encuentra la lista de plataformas soportadas y un montón de enlaces a los recursos más variados, como programas y las FAQ, además de una lista de programas ya listos (http://www.freebsd.org/applications.html) y las importadas de otras plataformas (http://www.freebsd.org/ports/index.html). En la dirección http://www.freebsd.org/projects/newbies.html existe un enlace previsto para los recién llegados que no saben nada de Unix o de FreeBSD.
Para recuperarlo se parte de http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/mirrors.html. Quien tenga una buena conexión a Internet puede instalarlo directamente desde la Red, a partir de un par de viejos discos floppy.



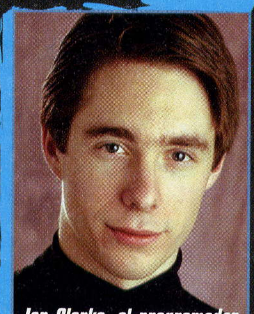




La red para compartir la información en libertad y en absoluto anonimato

TODOS MÁS LIBRES CON FREENET

Me preocupa mi hija e Internet cada vez más, aunque sea aún demasiado pequeña para conectarse. Me preocupa que dentro de diez o quince años vendrá y me dirá: papá, ¿dónde estabas cuando nos quitaron la libertad de expresión en Internet?
- Mike Godwin, Electronic Frontier Foundation

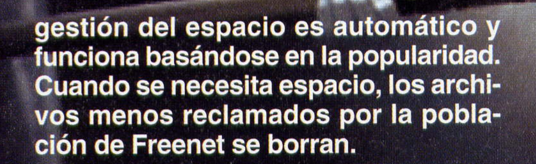

Ian Clarke, el programador que ha iniciado el proyecto Freenet. Ian está aún muy implicado en el proyecto, aunque el desarrollo full time ha sido asumido en gran parte por programadores nuevos.

Freenet es un software libre que permite leer y publicar en Internet información de modo seguro y libre de toda censura. El programa crea una red descentralizada de comunicación anónima, porque sin anonimato no puede haber verdadera libertad de expresión y la descentralización la hace menos vulnerable a ataques exteriores.

Parece la descripción de una típica red peer-to-peer, pero con una diferencia fundamental: en Freenet las comunicaciones están cifradas y van de nodo a nodo, para hacer muy difícil entender quién está pidiendo cierta información y de qué información se trata. En el p2p esta información es clara como el agua y todos saben qué descargamos.

Un esfuerzo colectivo

Quien participa en Freenet pone de su parte poniendo a disposición de la comunidad una porción de disco duro (la llamada data store) y de ancho de banda. ¿Cómo el p2p? En absoluto. La data store contiene archivos cifrados que ni el propietario del disco puede leer y ni controlar. El mecanismo de



gestión del espacio es automático y funciona basándose en la popularidad. Cuando se necesita espacio, los archivos menos reclamados por la población de Freenet se borran.

También a diferencia del p2p, Freenet puede ser usado en muchos otros modos además de compartir simplemente archivos. Su estructura es más semejante a la de una Internet dentro de Internet, tanto que es posible incluso publicar sitios Web (freesite) y abrir foros de discusión, además de distribuir contenidos.

Freenet es hoy un instrumento en vanguardia de la defensa de la libertad en Internet. El software ha sido descargado por más de tres millones de personas y para muchos, especialmente en naciones no libres como China o muchos de Oriente Medio, constituye un recurso insustituible, al que algunos deben hasta la seguridad física personal, si no la vida.

Contar con demasiados nodos de Freenet nunca será un problema, muy al contrario: siempre habrá demasiado pocos. Todo aquél que decide poner a disposición su parte de disco duro, lo hace para la libertad de todos y para un proyecto muy importante. ¡Si alguien lo hace, estamos interesados en saberlo!

The Freenet Project
http://freenetproject.org/

POR DÓNDE SE EMPIEZA

Para entrar en Freenet la página de inicio es http://freenet.sourceforge.net/index.php?page=download. Están disponibles los ejecutables para Windows y para Unix/Linux. Este último funciona también en Mac OS X, aunque hay que ser bastante bueno para efectuar algunos cambios en el archivo de shell de inicio de Freenet.
La primera vez que se inicia Freenet hay que esperar bastante, incluso algunos minutos. Es absolutamente normal y sirve para que el software encuentre y conecte a nuestro equipo otros nodos de la red. A partir del siguiente arranque todo será bastante más ágil.

EN EL CENTRO DE LA RED DESCENTRALIZADA

El hogar de Freenet es el sitio homónimo, en la dirección http://freenet.sourceforge.net. En el link Support se encuentra una serie de mailing list de actualizaciones, noticias, soporte y desarrollo, y hasta una línea de chat para hablar de Freenet en tiempo real. La página http://freenet.sourceforge.net/index.php?page=tools contiene una serie de utilidades que simplifican y agilizan la administración.

ECHAR MANO A PHP



Por sí solo el archivo php.ini funciona muy bien tal cual. Pero cada cual tiene sus preferencias, conoce sus trucos y prefiere configurar las cosas a su gusto. También para trabajar más deprisa. En diversas ocasiones se ha hablado de configurar php.ini y de modificar sus parámetros, pero las posibilidades son enormes. Veamos si conseguimos descubrir algún nuevo truco útil.

Las mejores rutas

Una variable del archivo php.ini llamada include_path sirve para configurar las rutas de búsqueda. Es como si cargáramos el sistema de navegación por satélite con los mapas de un país desconocido. Damos al sistema una serie de directivas de donde partir para descubrir lo necesario durante el funcionamiento. Luego, si no encuentra el camino correcto, de todos modos nos lo preguntará, pero primero habrá hecho todos los intentos entre los conocidos, que le hemos indicado mediante include_path, precisamente. Así, cuando php tenga que hacer referencia a archivos sin un path específico, una ruta, primero comprobará los directorios que le hemos indicado.

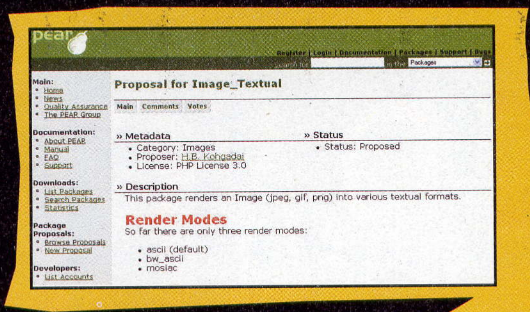
Si, por ejemplo, tenemos una serie de clases o de bibliotecas usadas con frecuencia, con include_path podemos listar las rutas para hallarlas sin ralentización del proceso. Otro truco útil: es el sitio justo para especificar las clases PEAR (Php Extension and Application Repository)



Cada cual tiene sus preferencias. ¡En el archivo php.ini está todo lo necesario para hacerlo funcionar a nuestra medida!

En el proyecto Pear se encuentran muchos proyectos interesantes, como uno para trasformar archivos .jpeg, .gif, .png en imágenes Ascii...





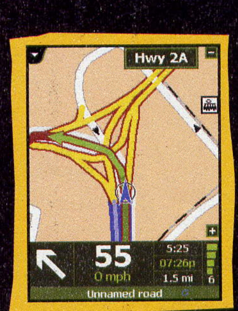
de php, que permiten escribir código limpio y normalizado. He aquí cómo escribir algo así:

```
include_path=
".:/usr/local/lib/php/pear:"
```

Atención usuarios de Windows: podemos especificar varias posiciones separándolas con punto y coma, a diferencia de los usuarios de Unix que tendrán que utilizar los dos puntos.

2 variables hermanas

Auto_prepend_file y auto_append_file son otras dos variables útiles para estas ocasiones. La primera sirve para pegar al principio de cualquier documento generado por php un encabezamiento. La segunda para pegar un pie de página. Son muy útiles para identificar bien con nuestros datos cualquier documento que generemos, sin vernos obligados a añadir cada vez unas líneas de código. Son interesantes sobre todo cuando estamos proyectando un servidor dedicado a una aplicación particular, porque los datos se adjuntan primero y después todos los documentos generados y esto puede ser inútil o hasta fastidioso.



El código lo podemos escribir como un script php simple e independiente, o anexionado en código HTML, encerrado entre las etiquetas <?php...?>:

```
auto_prepend_file =
/home/web/includes/header.php
auto_append_file =
/home/web/includes/footer.php
```

Administrar estupideces

Los errores que suelen producirse cuando se usa php son más o menos de cuatro tipos. El primero es lo que los anglosajones llaman "fatal error" y no necesita explicaciones. Cuando sucede ya es demasiado tarde y generalmente la aplicación se para: se bloquea y es necesario echar mano al código.

Los errores no fatales, o advertencias, así como los errores de código -como una variable no inicializada- y los errores de parsing -cuando una instrucción no se interpreta- son las otras posibilidades de errores que php nos señala con los avisos adecuados. Podemos hacer que estos avisos no se muestren, sino que se escriban en un archivo de log que podremos estudiar con calma después de haber probado la aplicación. Es interesante sobre todo en la fase de desarrollo. ¿Cómo hace? Capturamos los códigos de error con la variable:

```
error_reporting = E_ALL
```

y evitamos que aparezcan poniendo a off la variable

```
display_errors= off
```

Especificar el path es como mirar el mapa de nuestro navegador: hallar el camino será mucho más fácil.

En fin, es bueno y útil que los capturemos en un archivo de log, que puede especificarse con el valor syslog o con un nombre cualquiera, donde se recogerán las señales de error eventualmente generadas. En resumen, podemos escribir:

```
display_errors = Off
log_errors = On
error_log = "error.log"
```

A partir de ese momento, será necesario que vayamos a leer con regularidad el archivo error.log, para tener bien presente qué está sucediendo con nuestra aplicación. Allí estarán los problemas detectados.

HACERSE UN PEAR

Pear es un depósito de extensiones y aplicaciones para php que incluye:

- **una biblioteca** estructurada de código open-source para usuarios de php;
- **un sistema de distribución** del código de mantenimiento de las aplicaciones;
- **un estilo estándar** para la escritura de código php;
- **las clases fundamentales** de php;
- **algunas bibliotecas de extensiones;**
- **un sitio web,** un mailing list y sitios espejo para sostener la comunidad de desarrolladores en php

El sitio de referencia para el proyecto Pear es http://pear.php.net/

VULNERABILIDAD DE UN QUIOSCO

Desde hace unos años están presentes en muchos lugares, a menudo públicos, unos terminales llamados "quioscos", mediante los cuales es posible acceder a diversos servicios. Son ejemplos los instalados en las bibliotecas, útiles para acceder a los catálogos online para localizar libros y material multimedia. Estos terminales permiten el acceso a Internet de modo muy controlado. El administrador del quiosco tiene la facultad de permitir el acceso sólo a pocos y bien elegidos sitios, generalmente relacionados con el uso del quiosco o bien con servicios que se consideran de interés para el usuario. En el caso de las bibliotecas, si seguimos con el mismo ejemplo, es fácil hallar la posibilidad de acceso sólo a los sitios de entes públicos relacionados de alguna manera con el lugar donde el quiosco está instalado. Por ejemplo, es posible acceder al sitio institucional de la región, del municipio, o a alguna dirección de ministerios y asociaciones culturales, etcétera. La navegación libre en está casi siempre prohibida, porque el administrador del quiosco, como de cualquier otro punto de acceso a Internet abierto al público, tiene obligaciones legales que respetar, como son la exacta idenficación del usuario que está utilizando el equipo, para evitar o desalentar usos ilícitos (spamming, descarga de recursos ilegales, etcétera).

Un exploit imprevisto

Una gran cantidad de sistemas autónomos instalados en los lugares públicos se basan en SiteKiosk, un programa que se encuentra en la dirección www.sitekiosk.com, distribuido también en versión shareware; versión sobre la cual podemos hacer nuestras pruebas. En la práctica pue-

POR FIN EN RED

Los terminales-quiosco, en general, tienen una característica. No son verdaderos pc stand-alone, sino que están configurados para acceder en red todos al mismo disco duro. Por ello, en realidad, nuestra configuración se ha instalado en el disco duro del servidor central y una vez creada podremos usarla siempre, porque la encontraremos en cualquier terminal de cualquier sitio conectado al mismo servidor, sea cual sea.





Los quioscos informativos públicos son sistemas blindados que no permiten acceder a Internet libremente. ¿Pero seguro que han sido configurados correctamente? Porque en teoría es posible que...





de suceder que el programa en cuestión esté mal configurado y sin la atención debida. En particular, la configuración errónea del sistema utilizado para blindar el terminal hacia el exterior (¡=Internet!) y del sistema en general, permite crear nuevas configuraciones sin ninguna restricción y después abrir otra ventana con nuestra configuración, que evidentemente incluya el permiso de navegar tranquilos.

Una sesión alternativa

La cuestión, después de algunas pruebas hechas con el software e imaginando estar ante un terminal, puede ocurrir exactamente como la describimos. Si en la realidad nos damos cuenta de que efectivamente es posible actuar de este modo, tenemos que sentirnos obligados a advertir al administrador del quiosco, para que pueda tomar las medidas adecuadas, y reconfigure el sistema para que sea seguro.
Comprobamos que estamos en la página inicial con un un clic sobre "Start", presente en la barra superior central. Desde aquí seleccionamos uno de los iconos presentes. Generalmente, si por ejemplo estamos en una biblioteca, uno estará probablemente dedicado a los libros y otro a la sección multimedia. Estamos pues entrando en el sistema. Ahora seleccionamos un banner relativo a un sitio cuya visita esté permitida. Supongamos que es el de la región: en general siempre está, porque estos sistemas a menudo tienen esponsorización de organismos regionales. Dentro del sitio que hemos alcanzado buscamos cualquier documento descargable, por ejemplo un documento pdf. Para ello podemos usar la casilla de búsqueda, en general siempre presente en los sitios en cuestión. En el campo "buscar" es suficiente escribir "pdf" o ".pdf". Seleccionamos un resultado al azar entre los obtenidos. El fin de esto es acceder al disco duro del terminal. ¡Bien: se nos pregunta si queremos abrir el documento o guardarlo!
Un clic en guardar, luego un clic en "c:\" y vamos a Programas y a la carpeta SiteKiosk. Comprobamos que en el campo "Guardar como" dice "todos los archivos". Aparece también el archivo Configure.exe. Lo seleccionamos con un clic y con el botón secundario seleccionamos "Abrir". Evidentemente no tendremos permiso para modificar la configuración existente, ¡pero nada nos impide crear una configuración nueva a la medida de nuestros fines!
Sólo falta configurar nuestra ventana para el web. Recordad entre otras cosas mostrar la barra para la introducción del url y la tecla close para cerrar la ventana, luego damos un nombre a esta nueva configuración y la guardamos.
Para abrir otra ventana lanzamos Sitekiosk (en C: \Programas\SiteKiosk\ abrimos el archivo sitekiosk.exe, igual que hemos ejecutado configure.exe). Si aparecer algún pop-up de aviso basta un clic en Aceptar, hasta que salga la ventana que nos pedirá qué archivo de configuración usar. Seleccionamos nuestro archivo recién creado... Ya podemos navegar por Internet con el terminal de un quiosco, basado en SiteKiosk, mal configurado.

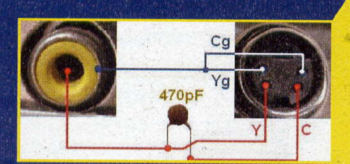


WebCam, televisor y PC: veamos en la TV si llega alguien

TV ANTI-INTRUSO



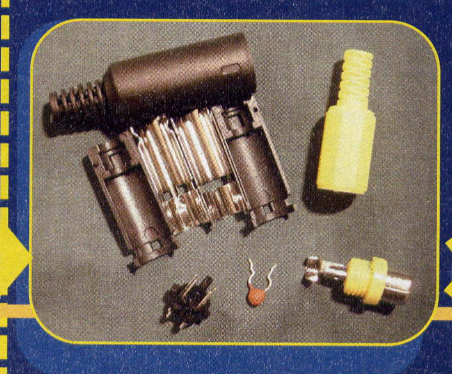
ESQUEMA



Esto es lo que vamos a construir. Se trata de unir la salida S-Video de la luminancia Y con la de crominancia C, con un pequeño condensador de 470pF.
Unimos también las dos masas: Yg y Cg (g es ground = masa).Los dos hilos así obtenidos se conectan, mediante cable, a la entrada amarilla del televisor, la entrada de vídeo. En este esquema hemos usado las fotografías de las tomas S-Video y RCA, para entender qué queremos obtener. La conexión S-Video que usaremos es un conector que, mirado por el lado de las soldaduras, tiene el terminal dispuesto como en la imagen.

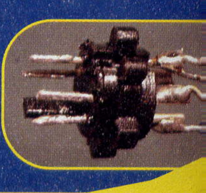
COMPOS

Los componentes: el conector S-Video, la toma RCA amarilla, el pequeño condensador cerámico de 470pF. El valor de la capacidad del condensador va escrito sobre su cuerpo de modo un poco extraño. En general como 471, donde 1 es el número de ceros después de las cifras 47.



SOLDADURAS

En el conector S-Video, por el lado de las soldaduras (los terminales más cortos) hay que conectar el condensador a los dos terminales más cercanos. Luego, mirando el conector teniendo hacia abajo los dos terminales vecinos, soldamos al de la izquierda uno de los hilos del cable, como en la imagen. Los otros dos terminales, más alejados, se unen entre sí y con el segundo hilo del cable. El mismo hilo hace de puente de unión: lo soldamos todo.

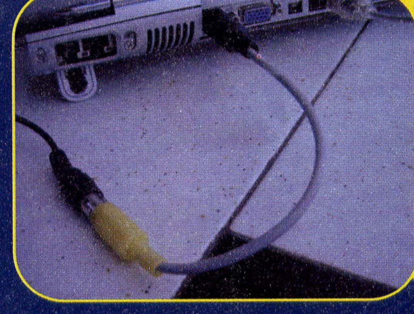




Cómo conseguirmos conectar nuestra WebCam USB al televisor? No es cosa simple, porque nuestra WebCam tiene una salida USB. Para complicar las cosas, nuestro portátil tiene solamente una salida de tipo S-Video para conectar un monitor externo, uno de esos conectores redondos de cuatro patillas.
Hemos buscado en nuestro televisor la correspondiente entrada, pero constatamos que no hay: el TV es un modelo económico, de gama baja.
En compensación encontramos una toma amarilla, redonda, de tipo RCA: la toma para la señal de video llamada compuesta.
¿Cómo poner de acuerdo las dos cosas? Simple: nos construímos un cable adaptador!

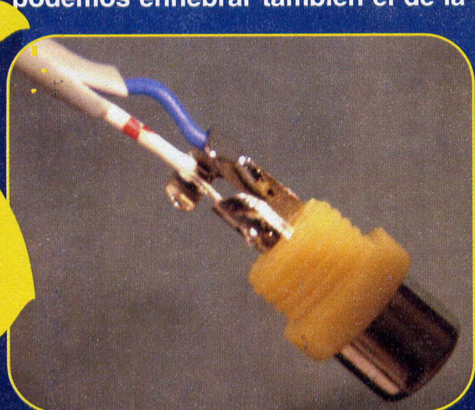
De S-Video a RCA

El cable se construye con pocos euros, un soldador, un poco de estaño y un poco de precisión, porque tenemos que trabajar sobre componentes muy pequeños.
Tenemos que conseguir:
una toma de s-video;
una toma de RCA;
un pedazo de unos veinte centímetros de largo de cable de dos hilos;
un cable RCA macho-macho de la longitud deseada (lo compramos ya hecho, acabaremos antes);
un condensador cerámico de 470pF;
Todos son componentes que encontraremos en cualquier tienda de material electrónico.



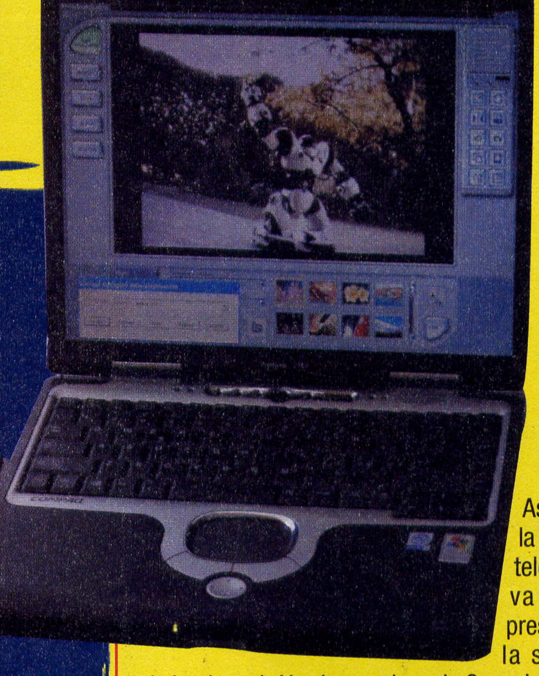
Seguir Soldando

En el otro cabo del corto cable tiene que soldarse la toma RCA. Antes de hacerlo recuerda que debes hacer pasar el hilo por el tope de la toma que lo cubrirá todo. Aún podemos enhebrar también el de la conexión S-Video, si no lo hemos hecho aún. El terminal central se conecta al hilo proveniente del condensador. A la masa lateral se conecta el hilo proveniente de los dos terminales de masa, que habíamos unido en el conector de S-Video.



Cómo funciona Y y C

Entre nuestros aparatos, por ejemplo el PC y el TV, transferimos la señal de vídeo de modo "compuesto". En realidad en origen las telecámaras a color toman las imagenes en tres colores fundamentales: rojo, verde y azul, en una señal llamada RGB. De los colores fundamentales, por suma o resta, derivan todos los demás colores. Para hacer compatible RGB con los viejos televisores en blanco y negro, un circuito suma los tres colores en porcentajes diversos y fijos (0.30 R + 0.59 G + 0.11 B), estudiados sobre el hecho que una tonalidad "se ve" más que otra (supongamos que pintamos una bombilla de amarillo y otra de azul, con la misma cantidad de pintura: ¿cuál da la sensación de dar más luz?). La señal que resulta se llama luminancia y contiene toda la imagen, pero sólo como variación de luminosidad entre un punto y otro. Perfecto para un televisor en blanco y negro, al que se puede enviar sólo Y para ver la imagen. Para los aparatos a color tenemos que añadir la señal C, de crominancia. Se construye restando B a la luminancia y R a la luminancia (B-Y e R-Y).

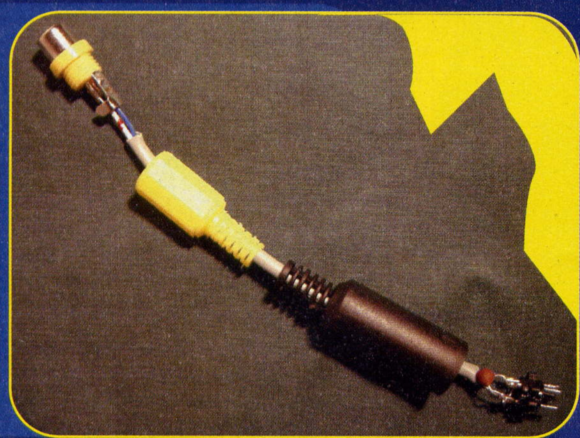


Así, en la señal televisiva está presente la señal de luminancia Y y de crominancia C, por las dos restas. ¿Y el color que falta? No se transmite, sino que se obtiene por diferencia entre los porcentajes que hemos visto antes. Si tenemos los porcentajes de B y R, el verde G lo obtenemos por diferencia de 100. Es lo que hace nuestro televisor cuando le enviamos Y y C: tiene todos los datos necesarios para reconstruir la imagen y su color.

CABLE

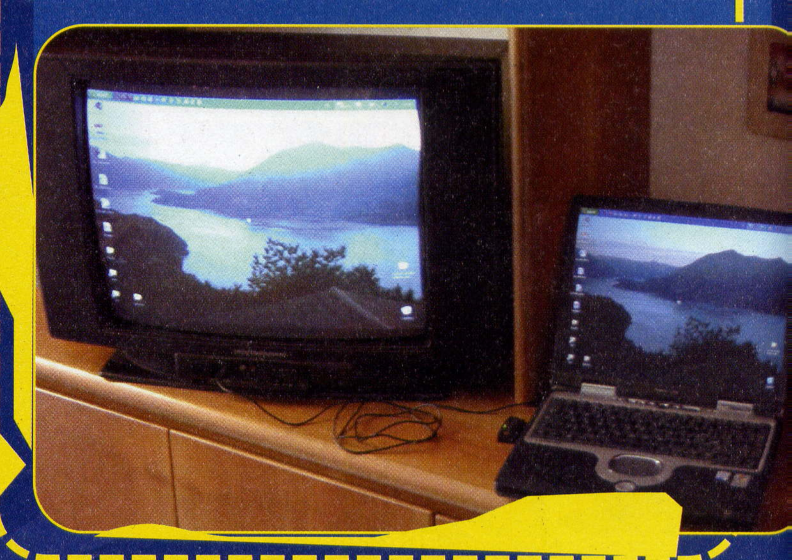
El cable tiene este aspecto, antes de cerrar los topes. Como se ve, las dimensiones del condensador permiten insertarlo tranquilamente dentro del mismo capuchón.





FINAL

He aquí nuestro equipo portátil conectado al televisor. Mediante un cable RCA macho-macho hemos conectado la toma del televisor a la toma de nuestro cable autoconstruido. Un óptimo accesorio a tener siempre a mano, para resolver fácilmente situaciones en las que se quiera ver imágenes en cualquier televisor que tengamos a mano, aunque no sea un último modelo.



WEBCAM

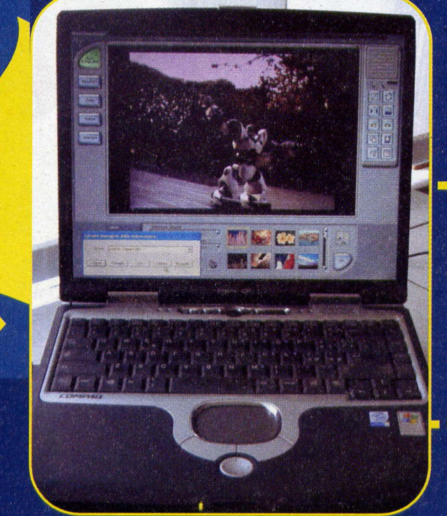
Nuestra webcam está controlando el camino exterior: si alguien vuelve a casa mientras simulamos estudiar, lo vemos inmediatamente en la pantalla del TV.



INTRUSOTV

¡Atención! Un intruso en actitud amenazadora se acerca a la casa! ¡Alarma!





INTRUSOPC

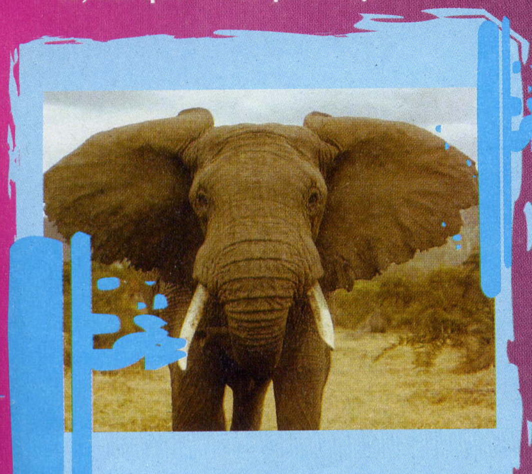
Todo lo que vemos en la pantalla del PC lo podemos ver a la vez también en un televisor.

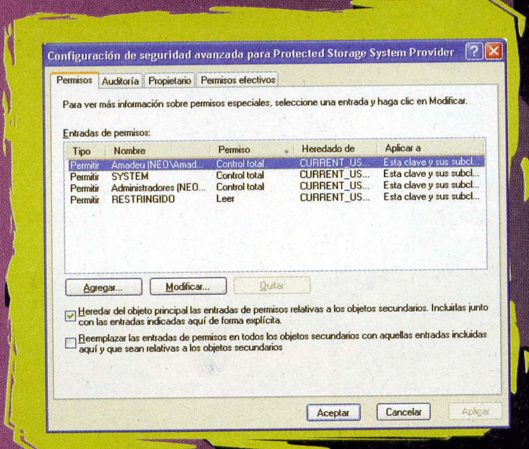


CUANDO OUTLOOK PIERDE LA MEMORIA

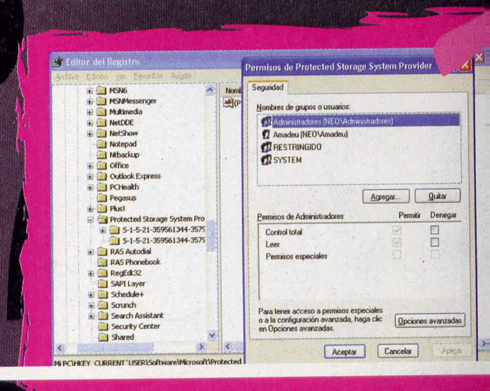
Outlook olvida los passwords y cada vez tenemos que reinsertarlos todos

Nada es más fastidioso que cuando Outlook olvida las contraseñas que hemos insertado, con toda la paciencia, en cada cuenta. A pesar de decirle que las memorice, no las recuerda y sigue pidiéndolas. Parece que no haya remedio, pero no es así. Basta seguir este procedimiento, que entra en las profundidades de regedit. Atención: los nombres de los menús pueden cambiar ligeramente según la versión de Windows que se esté usando. Pero las diferencias se resuelven fácilmente, así que no os preocupéis.





Paso 1) Cerrar todos los programas en ejecución.
Paso 2) Inicio > Ejecutar escribir regedit y después un clic en Aceptar
Paso 3) Buscar la subclave del registro: HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider
y hacer clic en Protected Storage System Provider
Paso 4) Escoger Permisos del menú Cambiar
Paso 5) En la ventana Permisos de Protected Storage System Provider hacer clic en Opciones avanzadas en el apartado Permisos.
Paso 6) En la ventana "Configuración de seguridad avanzada para Protected Storage System Provider" seleccionar la casilla de control "Heredar del objeto principal las entradas de permisos relativas a los objetos secundarios" y clic en Aceptar.
Paso 7) Escoger Sí cuando aparece un mensaje parecido a éste:
"En este modo se eliminarán los permisos definidos explícitamente para todos los objetos heredados y se habilitará la propagación de permisos heredables de los objetos heredados. Sólo los permisos heredables propagados por Protected Storage System Provider tendrán efecto. ¿Continuar?"
Paso 8) Un clic en todos los Aceptar hasta volver al editor de registro del sistema. Con un doble clic ampliar Protected Storage System Provider, seleccionar la carpeta subclave de usuario (cuyo nombre normalmente empieza con la letra S y está compuesto por una larga serie de números separados por guiones), luego pulsar Esc, para borrarlo.
Paso 9) Si el PC lo usan diversos usuarios y todos tienen el mismo problema, eliminar la carpeta de subclave de los usuarios. Así no se eliminan las cuentas, sino sólo los permisos relativos a las contraseñas.
Paso 9) Clic en Salir del Registro del sistema, después reiniciar el PC.
Paso 10) Una vez reiniciado, seleccionar Inicio > Panel de control > correo electrónico, luego Ver perfiles y sobre Propiedades para la cuenta de Internet seleccionada. Se vuelve a escribir la contraseña y seleccionamos la opción Guardar contraseña, después Aplicar y Aceptar.
¡Ahora todo va bien!





PAD ANTICENSURA

Un sistema simple e ingenioso para proteger información de qualquier mirada indiscreta.

La libertad de palabra y de pensamiento es un bien muy importante y la censura es una grave amenaza. ¿Cómo asegurar que nuestro pensamiento puede permanecer en la red evitando cualquier censura?

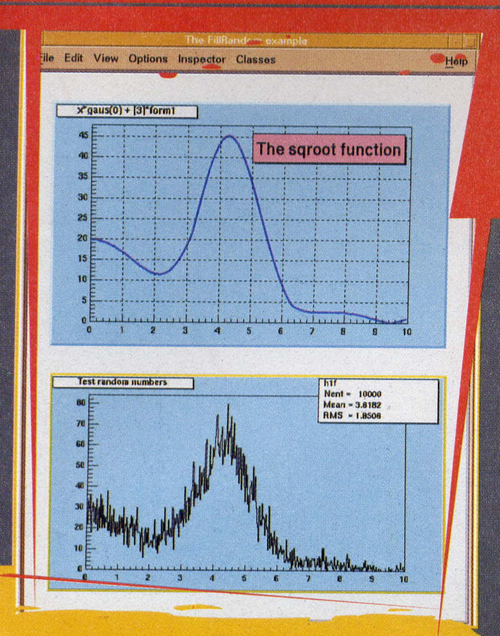
Un mundo de pads

Supongamos que cada uno de nosotros conserva en su PC campos de datos al azar. Los llamamos pad. Cada pad contiene, por ejemplo, 128K de bits tomados completamente al azar.

A cada pad le damos un nombre unívoco, que no se confunda con otros. Una buena convención puede ser por ejemplo pad-md5-629755a24a76cf0e486b76fc2b848436.dat, donde pad y md5 son fijos y los 32 caracteres siguientes corresponden al denominado digest de los datos según el sistema MD5. Éste asegura que en la práctica será imposible, o casi, que dos pads tengan el mismo nombre de archivo.

Cada pad tiene que estar replicado todo lo posible en Internet, pero cada sitio particular tiene que contener sólo un pequeño número de pads.

En los pads hay bits casuales pero, mágicamente, si combinamos varios



La producción de números casuales es importante para tener información capaz de escapar a cualquier censura.

pads a través de una función XOR se obtienen datos reales, guardados dentro del propio pad. Es importante notar tres cosas: primero, ningún pad contiene todos los datos de la información real, sólo una parte; segundo, el propietario de un pad puede no saber qué hay dentro; tercero, a falta de más información, el contenido de un pad es perfectamente indistinguible de un campo de datos casuales.

Cómo hacerlo

Crear un pad no es complicado. Se requieren 128K de datos al azar. Se requieren más pads (al menos tres, mejor cinco, como máximo siete, para la mayor seguridad y eficiencia) tomados por Internet y producidos por otras personas. Tomamos los datos que queremos asegurar y hacemos un XOR con los pads, usando por ejemplo Perl. De los pads cruzados obtenemos un nuevo pad, compuesto por nuevos caracteres, siempre casuales. Pero, si hacemos otro XOR con el pad primitivo, obtenemos el trozo de archivo que habíamos escondido. El resultado tiene que



ser llamado con un nombre de archivo que siga las mismas convenciones que los demás, así que es imposible distinguirlo.

Recoser los trozos

Alguien, en la red generada, debe conservar las listas de nombres de pads que, juntos, generan cierto archivo. Ese alguien, posiblemente, tiene que conservar pocos pads o ninguno. Para recuperar el archivo se busca en la red la lista de nombres, luego los pads correspondientes y se reúne todo con el programa adecuado.

LA LISTA DE LA COMPRA

Lo necesario para empezar está todo aquí:
El script Perl para reunir los pads: ftp://quatramaran.ens.fr/pub/madore/PADS/xorpads.pl.
Otro script Perl utilizable: ftp://quatramaran.ens.fr/pub/madore/PADS/contrib/xorpads2.pl.
Programa Delphi para Windows que genera pads random y efectúa XOR: XORFiles.zip del directorio ftp://quatramaran.ens.fr/pub/madore/PADS/contrib/ (¡mirarlo todo!).
Pad de prueba: en el apartado Sample Pads de la página http://www.eleves.ens.fr:8080/home/madore/misc/freespeech.html.
Pad ya listos: por ejemplo http://adware.no/randompads, http://hem.passagen.se/vildman/pads/, http://users.cybercity. dk/%7eccc48268/. Hay una lista más larga (pero algunos links no funcionan) en el apartado Known Pad Repositories de la página http://www.eleves.ens.fr:8080/home/madore/misc/freespeech.html.





UNA PREGUNTA CON TRAMPA

Todo lo dicho es sólo teoría; quien usa el sistema de pads para violar la ley es un tonto, como mínimo. Pero supongamos que tenemos el archivo de una película, partido en varios pads. Cada pad contiene de hecho datos que no son directamente los de la película y cada PC contiene sólo un trozo de lo necesario para reconstruir la película. ¿Cómo se puede acusar al poseedor de un pad de violación del copyright?

Los pads inocentes

Un pad inocente sirve para enturbiar las aguas. Sus datos parecen azarosos pero no lo son, y el contenido es, precisamente, inocente. Algunos ejemplos:

- **concatenar los digest MD5** de todos con la Divina Comedia, con la Biblia u otra obra de dominio público;
- **cruzar con XOR las cifras, en binario,** de pi y de la raíz cuadrada de 2;
- **tomar una foto de familia** y cifrarla con cualquier sistema, también banal.

Un pad inocente sirve también para probar la propia inocencia, por cuanto es fácil mostrar de qué se trata y cómo se ha generado.

Si se crea un montón de pads, muchos con datos al azar, alguno inocente y otros con información útil disfrazados con XOR, estos últimos serán razonablemente seguros .

¿Quién comienza a crear pads? Si somos suficientes, lo conseguiremos...

CYBERENIGMA:
HECHOS EN SERIE

EMPEZAMOS POR UN NÚMERO. SI EL NÚMERO ES PAR, LO DIVIDIMOS POR LA MITAD. SI ES IMPAR, LO MULTIPLICAMOS POR 3 Y SUMAMOS 1. EMPEZAMOS POR EL NÚMERO 1.

1 es impar, así que multiplicamos por 3 y sumamos 1: 1 * 3 + 1 = 4.

4 es par, lo dividimos por 2: 4 / 2 = 2.

2 es par, lo dividimos por 2: 2 / 2 = 1.

La serie ha llegado a 1 y se cierra (si continuamos, se repite continuamente), en tres pasos.

PARA TODOS: en cuantos pasos se llega a 1 si se empieza por el número 27? Se puede hacer a mano, con una hoja de cálculo, o hallar un sitio que nos lo haga... la serie se llama 3n+1. También toma el nombre de la conjetura de un matemático...

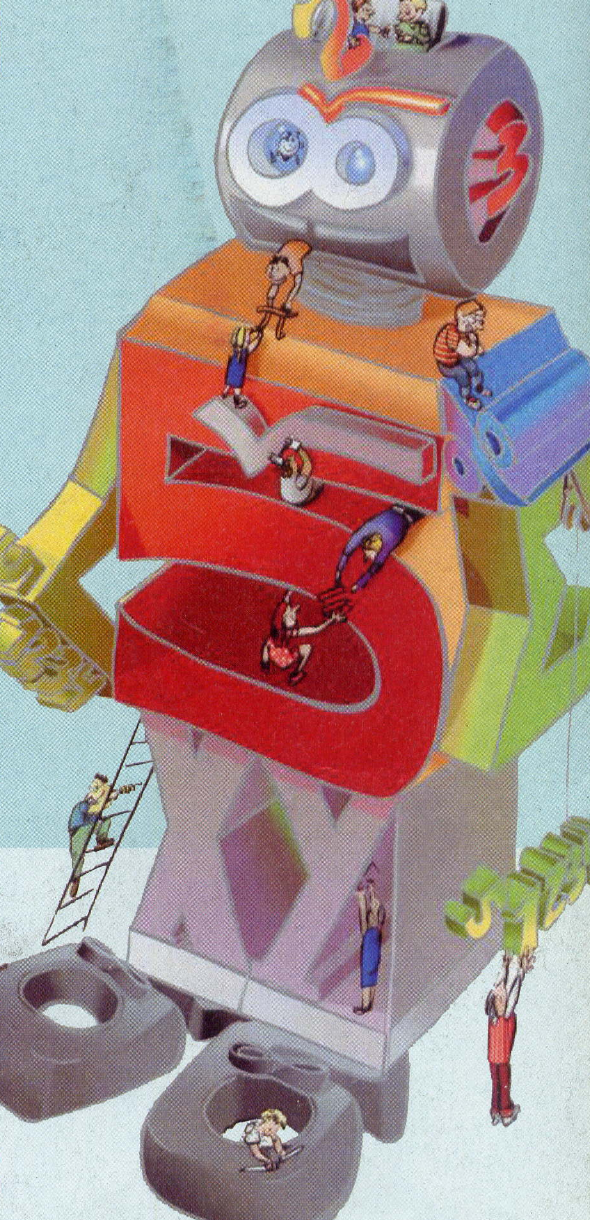
¿Para qué sirven estas cosas? Podemos usar esta regla para comunicar un mensaje cifrado. Si tomamos el número 6 y ponemos en fila todos los números generados por la regla, tenemos 63105168421 (6-3-10-5-16-8-4-2-1), que puede ser la clave de un pad. Le decimos al destinatario "6", y ya sabe qué hacer (el resto, no).

PARA EXPERTOS: la clave es 132113213 221133112132123222110. Para llegar a ella, hemos hecho lo siguiente:

0
10
1110
3110
132110
1113122110
311311222110
13211321322110
1113122113121113222110
31131122211311123113322110

¿Cuál es la regla?
Una pequeña pista: no veremos nunca un 4 y el cero puede encontrarse sólo a la derecha. Si en lugar de por 0 la serie empezara por 1, ¿cómo sería?

PARA SÚPER HACKERS: escribir un programa que acepte un número y con él reproduzca los pasos de la serie 3n+1, contando los pasos que se dan para volver a 1 (bastante fácil). O bien, escribir un programa que produzca por sí solo o por un número de pasos arbritrario la serie para expertos, aplicando la regla adecuada (más complejo). ¿Conseguimos encontrar una regla muy simple que produzca una serie interesante, como por ejemplo 0110100110010110 01011001101001?



¡Nos vemos en el próximo número de Hacker Journal!